NAVAL POSTGRADUATE SCHOOL
Monterey, California

THESIS

COGNITIVE PASSWORDS:
THE KEY FOR EFFECTIVE ACCESS CONTROL

by

JOHN DOUGLAS HULSEY

SEPTEMBER 1989

Thesis Advisor: Moshe Zviran

REPORT DOCUMENTATION PAGE

REPORT SECURITY CLASSIFICATION UNCLASSIFIED	1b RESTRICTIVE MARKINGS
SECURITY CLASSIFICATION AUTHORITY	3 DISTRIBUTION/AVAILABILITY OF REPORT Approved for public release; distribution is unlimited.
DECLASSIFICATION DOWNGRADING SCHEDULE	
PERFORMING ORGANIZATION REPORT NUMBER(S)	5 MONITORING ORGANIZATION REPORT NUMBER(S)
NAME OF PERFORMING ORGANIZATION Naval Postgraduate School 6b OFFICE SYMBOL (If applicable) 367	7a NAME OF MONITORING ORGANIZATION Naval Postgraduate School
ADDRESS (City, State, and ZIP Code) Monterey, CA 93943-5000	7b ADDRESS (City, State, and ZIP Code) Monterey, CA 93943-5000
NAME OF FUNDING/SPONSORING ORGANIZATION 8b OFFICE SYMBOL (If applicable)	9 PROCUREMENT INSTRUMENT IDENTIFICATION NUMBER
ADDRESS (City, State, and ZIP Code)	10 SOURCE OF FUNDING NUMBERS PROGRAM ELEMENT NO / PROJECT NO / TASK NO / WORK UNIT ACCESSION NO

TITLE (Include Security Classification)

COGNITIVE PASSWORDS: THE KEY FOR EFFECTIVE ACCESS CONTROL

PERSONAL AUTHOR(S)
Hulsey, John D.

TYPE OF REPORT	13b TIME COVERED	14 DATE OF REPORT (Year, Month, Day)	15 PAGE COUNT
ster's Thesis	FROM ______ TO ______	September, 1989	110

SUPPLEMENTARY NOTATION

Approved for public release; distribution is unlimited.

COSATI CODES			18 SUBJECT TERMS (Continue on reverse if necessary and identify by block number)
FIELD	GROUP	SUB-GROUP	Computer Security; Access Control; Passwords; Cognitive Passwords

ABSTRACT (Continue on reverse if necessary and identify by block number)

Passwords are a commonly used method of access control for computer ystems. Traditional passwords have been found to be inadequate. Passwords are enerated from two sources: users and computer systems. User-selected asswords are easy to remember, but they might be easily guessed and therefore ield a lower degree of security. System-generated passwords usually offer a igher degree of security, but they are hard to remember and therefore meet ith high user resistance. Because of this user resistance, password systems re either circumvented or not used. A solution to this tradeoff between emorability and security is a security mechanism that is easily remembered, ser friendly, hard to guess and yields a high degree of security. Cognitive asswords offer these advantages. They are based on a series of predetermined uestions with answers known normally only by a specific user. Research into he underlying theory, types of applicable questions and implementation of a rototype system is conducted.

DISTRIBUTION/AVAILABILITY OF ABSTRACT ☒ UNCLASSIFIED/UNLIMITED ☐ SAME AS RPT ☐ DTIC USERS	21 ABSTRACT SECURITY CLASSIFICATION Unclassified
NAME OF RESPONSIBLE INDIVIDUAL Zviran, Moshe	22b TELEPHONE (Include Area Code) (408)646-2489 22c OFFICE SYMBOL 54ZV

Approved for public release; distribution is unlimited.

COGNITIVE PASSWORDS: THE KEY FOR EFFECTIVE ACCESS CONTROL

by

John D. Hulsey
Lieutenant, United States Naval Reserve
B.B.A., Georgia State University, 1975

Submitted in partial fulfillment
of the requirements for the degree of

MASTER OF SCIENCE IN INFORMATION SYSTEMS

from the

NAVAL POSTGRADUATE SCHOOL
SEPTEMBER 1989

ABSTRACT

Passwords are a commonly used method of access control for computer systems. Traditional passwords have been found to be inadequate. Passwords are generated from two sources: users and computer systems. User-selected passwords are easy to remember, but they might be easily guessed and therefore yield a lower degree of security. System-generated passwords usually offer a higher degree of security, but they are hard to remember and therefore meet with high user resistance. Because of this user resistance, password systems are either circumvented or not used. A solution to this tradeoff between memorability and security is a security mechanism that is easily remembered, user friendly, hard to guess and yields a high degree of security. Cognitive passwords offer these advantages. They are based on a series of predetermined questions with answers known normally only by a specific user. Research into the underlying theory, types of applicable questions and implementation of a prototype system is conducted.

TABLE OF CONTENTS

I. INTRODUCTION

A. THE NEED TO PROTECT COMPUTER RESOURCES

Concerns of privacy, proprietary interests, administrative confidentiality and, in the military, national security are considerations in the development of computer security systems. (Barton, et al., 1984)

Computer resources are vulnerable to compromise and attack for four reasons:

1. hardware may contain capabilities not originally designed,
2. an operating system may contain errors or capabilities that allow a user to deceive or circumvent a security system,
3. a security mechanism may contain errors or capabilities that can be exploited or circumvented,
4. poor password systems may lead to guessing of passwords by system intruders. (Kaiser, 1987)

The penalties for inadequate computer security are severe. Consequences of intrusion may include alteration, disclosure or loss of data of an entire system. Statistical evidence indicates that most unauthorized access attempts go unnoticed. One out of 100 computer crimes is detected. Of those crimes detected, one out of 22,000 is prosecuted. Of the computer crimes prosecuted, one out of thirty three leads to a conviction. (Hagopian, 1987)

Computer security ranges from physical security of buildings housing computer facilities to authentication of persons attempting to use specific application programs. The National Computer Security Center (NCSC), charged with the responsibility of

designing computer security systems for the United States government, equates security with trustworthiness (Kaiser, 1987). The NCSC defines trustworthiness as having four characteristics:

1. a security mechanism is fully integrated into the fiber of a computer system;
2. a system is robust, well-behaved and understandable;
3. a security mechanism is software-managed and hardware-enforced;
4. any change to an access permissions matrix is immediately enforced. (Kaiser, 1987)

The development of networks created the capability to communicate remotely with other computers. Physical restrictions no longer were adequate. Additional security mechanisms were needed to ensure the availability of widely dispersed systems while at the same time ensuring that only authorized people could gain access. Physical boundaries were replaced by electronic boundaries. A secondary security mechanism, passwords, came to the forefront. Passwords were thought to be inexpensive, easy to use and provide a level of assurance that the user was indeed authorized to use a computer system. Through the years, passwords were found to be lacking. Passwords that yielded a high degree of security were found to be hard to remember. Conversely, passwords that were easy to remember were found to yield a low degree of security (Barton, et al.,1984).

A continuing search for a better password system has led to the development of cognitive passwords. This thesis focuses on the feasibility, advantages, disadvantages and problems inherent in the use of cognitive passwords as a security mechanism.

After investigating the characteristics of the cognitive password approach and comparing them to the characteristics of the traditional password approach, a prototype will be developed to test and demonstrate the concepts and knowledge resulting from this investigation.

II. COMPUTER SECURITY: AN OVERVIEW

A. BACKGROUND

1. Computer Security: Definition

Computer security is a comprehensive strategy to protect and safeguard resources (Wood, 1983). Protective measures take the following sequence:

1. protect terminal locations;
2. limit the users that can activate a terminal through use of terminal keys;
3. use passwords to control user access;
4. use passwords to limit access to data resources;
5. require additional passwords for specific resources, such as programs and databases;
6. provide extra protection for sensitive data through encryption (Ahituv, et al., 1987).

Computer-based information systems are comprised of six major categories of resources: hardware, software, communication facilities, data, information and people. Each of these resources, either singularly or in combination, may be vulnerable themselves or be the means by which compromise is achieved.

Two general approaches may be used in developing a security system: all resources are protected or no resources are protected unless of a critical nature

(Wood, 1983). Some information managers emphasize the value of computer hardware rather than the value of the information stored in the system (Wood, 1983).

2. Protection Versus Accessibility

At one extreme, a security system might limit access to only one or two people. However, the benefit of information availability organization-wide would be lost. The net result would be a secure but useless system. At the other extreme, if no protection is afforded, accessibility would be high but system security would be lost. Computer security must be balanced between protection and accessibility. Figure 2-1 illustrates this tradeoff.

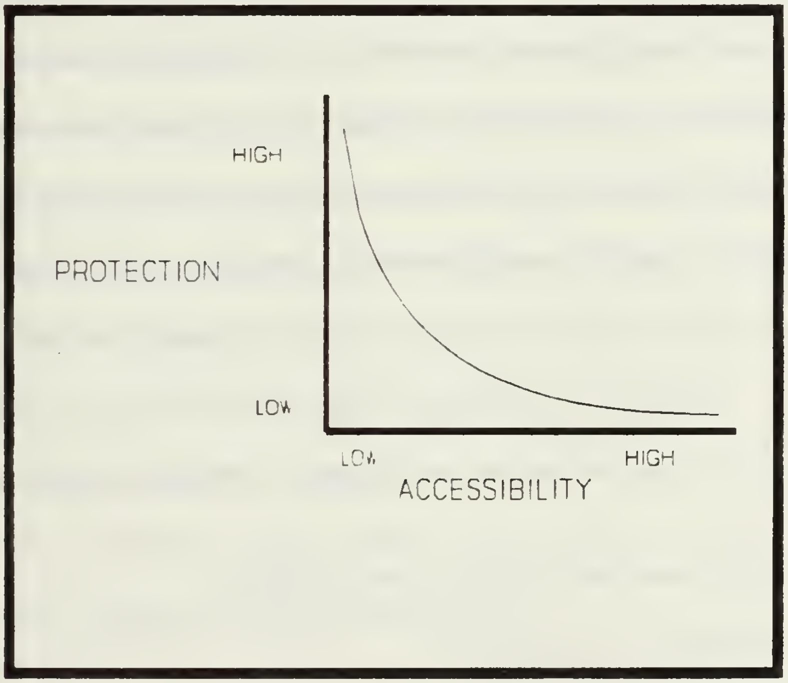

FIGURE 2-1
PROTECTION ACCESSIBILITY TRADEOFF

Two additional considerations of the protection versus accessibility tradeoff are cost and effect on the organization. As the degree of security rises, the complexity of protection increases, adding to costs. The cost of a secure system must be evaluated against the importance of the computer resource that is being protected. If the loss of a computer system could threaten the survivability of an organization, more funds are likely to be spent to protect the system. If, on the other hand, the loss of a system would have minimal effect, an organization may elect to implement only basic security measures.

The impact of the security system on an organization's personnel will also be important to an organization. Paans and Herschberg (1987) draw a correlation between security and the happiness of personnel. They indicate that implementation of security measures is viewed as the withdrawal of privileges and may even lead to potential sabotage. People can no longer enter certain areas without permission. In addition, they can not browse through databases unless they are specifically authorized access. Hagopian (1987) identifies four ways in which computer security will affect an organization:

1. additional job responsibilities are assigned causing possible organizational friction;
2. the security system makes sign-on more difficult;
3. access to resources are restricted;
4. the choice of which terminal to use will be reduced.

3. Types of Risk Exposure

Exposure represents possible loss or harm. Vulnerability is a weakness that might be exploited (Pfleeger, 1989). Types of exposures and vulnerabilities fall into six categories:

1. accidental disclosure
2. intentional disclosure
3. accidental modification
4. intentional modification
5. accidental destruction
6. intentional destruction (Fisher, 1984).

Disclosure, the sharing of information; modification, the changing of information and destruction, the elimination of information, require special control measures. Through security control measures, the exposures or vulnerabilities can be prevented, detected and corrected (Fisher, 1984). Pfleeger (1989) categorizes vulnerabilities into four threats:

1. interruption, an asset becomes lost, unavailable or unusable;
2. interception, an unauthorized party gains access;
3. modification, someone tampers with an asset;
4. fabrication, creation of spurious transactions.

4. CAUSES OF EXPOSURES

Fisher (1984) states six major causes of exposure: people, hardware, software, communications, procedures and acts of God.

a. People

Through curiosity or malicious intent, people are a major cause of exposure.

b. Hardware

Hardware-related exposures may be caused by inadequate or incorrect microcoding causing a legitimate request for information to yield an unauthorized set of information.

c. Software

The use of software to reveal information is probably the second major cause of exposures. During software development, a common practice is to implement specific ways for a developer to quickly gain access to certain segments of a program. These quick-entry mechanisms or "back doors" may not be completely eliminated before a program is released to users, allowing intruders to gain access to and modify original code.

d. Communications

With the proliferation of personal computers and their ability to communicate with other computer systems from anywhere in the world, the complexity of communications security is a significant problem. No longer can a security manager confidently establish boundaries around a system. Any person with a personal

computer, a modem, a communications package and some knowledge of an authorized password can gain access to a system.

e. Procedures

Procedures that have been poorly thought out can have detrimental effects. A payroll department procedure that allows the same employee to enter personnel into the payroll system and to authorize payroll checks may result in checks being issued to nonexistent personnel.

f. Acts of God

Acts of God include natural disasters such as floods, hurricanes or fires and can result in the loss of facilities and data. Backup and recovery procedures plus establishment of a geographically separated secondary facility can alleviate these possibilities.

5. SUMMARY

Figure 2-2 summarizes the relationships between causes and types of exposures and computer-based vulnerable resources.

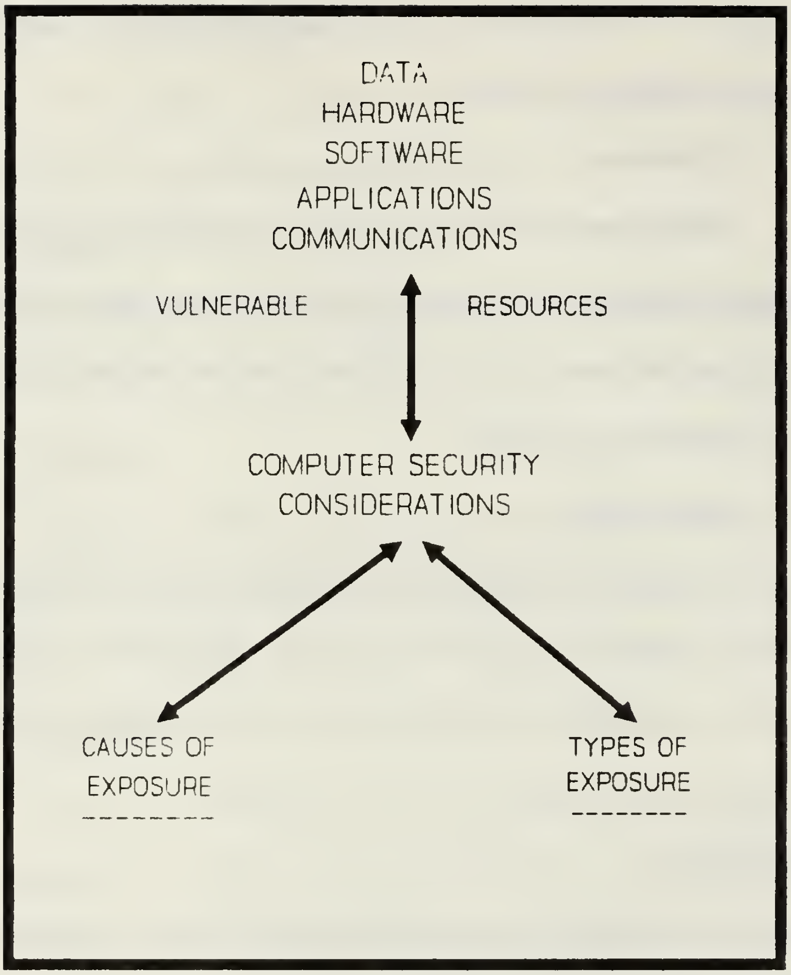

FIGURE 2-2

B. METHODS OF DEFENSE

Protection of computer-based information systems may be thought of as a layered approach. Each layer uses a different methodology to address the problems unique to that particular layer. The synergism of multiple layers may create a security system that protects its resources.

1. Types of Defenses

Hsiao, Kerr and Madnick (1979) delineate five types of defenses: operational security, physical security, hardware security, cryptographic transformations and operating system security.

a. Operational Security

The broad category of operational security encompasses two major areas: operating environment and authorization control (Hsiao, et al., 1979).

(1) Operating Environment. An operating environment is defined in terms of the degree of access allowed to a computer system. Three possibilities exist: closed, open or unlimited (Hsiao, et al., 1979). In a closed system only a few users have access. In an open system, any person can gain access by identifying himself or herself personally to another person authorized to grant access. In an unlimited environment, any person can gain access with little effort.

(2) Authorization Control. Authority to grant access to a system can be divided into three categories: centralized, hierarchial decentralized and individual (Hsiao, et al., 1979). Under centralized control, a person or department controls who is granted authorization. In hierarchial decentralization, functional managers have the power to grant access for specific areas under their control. The complete decentralization of control results in individual control: an owner of information is responsible to control access to it.

Authorization control or authentication can take many forms from passwords to the confirmation of biological traits. Various types of authorization control are discussed later in this paper.

b. *Physical Security*

Physical security encompasses acts of God, man-made disasters and intrusion (Hsiao, et al., 1979). Acts of God, such as fires and floods, may be controlled by installation of sensors and automatic suppressant systems such as a HALON 1211 fire fighting system. Man-made disasters or equipment failures such as a disk head crash can be minimized through a backup and recovery system. Intrusion, either intentional or unintentional, is a primary concern of physical security. Prior to the proliferation of network communications systems, avoiding intrusion meant keeping a person from physically entering a computer facility. With the current ability to access a computer through remote terminals, physical security must now be concerned with preventing access through communications media. Cipher locks, identification cards and door monitors are examples of tools used for physical security.

c. *Hardware Security*

Closely related to the design of hardware is the design of the hardware security system. Various hardware components require protection from both the user and computer applications or processes desiring to use the hardware resources. Examples of tools used are special microchips called registers and operating system software.

d. Cryptographic Transformations

A different approach to security is the encoding of user access information. The underlying assumption is that intruders will be able to gain access. Rather than try to prevent access, emphasis is placed on encrypting or scrambling the data making it unusable by outsiders (Hsiao, et al., 1979). Data that can not be interpreted are of little value. Tools commonly used are encryption and decryption algorithms.

e. Operating System Security

An operating system is the master program that controls the execution of all other processes and stays resident in main memory. Prior to the running of an application program, an operating system must be executed. An operating system acts as the mediator between competing processes and allocates resources based on demands. Gaining access to an operating system can lead to access of other programs. Advanced operating systems, such as UNIX, contain security components that can be activated.

C. DEFENSE TOOLS

The two major defense tools used in computer security are encryption and authentication (Wood, 1983).

1. Encryption

Encryption is accomplished by three methods: encrypting a password table stored in memory, using one-way encrypted passwords and using a personal key device that contains an encrypted code after the plain text password has been entered (Ahituv, et al., 1987). Encryption raises the effort required to break the code (Menkus, 1988).

2. Authentication

The most widely used defense tool is use of authentication methods. Identification by authentication is approached in two ways: use of natural properties, such as fingerprints, or use of artificial measures, such as passwords or magnetic cards (Ahituv, et al., 1987). Authentication methods use something known (a password), something possessed (a personal key), something to be performed (a signature) or some biological trait (a fingerprint) (Fisher, 1984).

The underlying logic of authentication devices takes two forms: make computers more like people by equipping them with biometric readers or make people more like computers by equipping them with personal computerized authentication devices (Spender, 1987). Authentication devices take the form of biometrics, directly connected token reading devices (keyholes which accept electronic keys), user interface tokens (pocket devices that can generate one-time passwords) and fixed password devices (plastic cards that contain access codes read electronically) (Spender, 1987).

More common than authentication devices are passwords, a group of characters that identify a user. With this background in computer security, Chapter III explores the use of passwords as a security mechanism.

III. PASSWORDS AS A SECURITY MECHANISM

A. DEFINITION

The risk of granting access to an invalid user must be measured against the cost of designing, implementing and maintaining an adequate security system.
Martin (1973) states that two types of errors may be possible: a false rejection in which the person is actually a valid user and a false acceptance in which access is granted to an imposter.

Passwords consist of a sequence of letters, numbers, special symbols or control characters used to authenticate a user's identity (Wood, 1983).

B. WHY USE PASSWORDS?

The use of passwords is the second oldest method of access control. In the early years of computer usage, the number of personnel authorized access was small. Each valid user was normally known to other users, and as such, an intruder could be easily identified. Prior to the development of networks and remote terminal capabilities, computer hardware was centrally located. Operators were the only users authorized access and they would have to be physically present in the computer room to communicate with the hardware. Password protection consisted of system passwords known to the group of operators.

The advent of networks and end-user computing brought computer resources out from under the centrally protected facility. A rudimentary password architecture became the answer to the problem of protecting dispersed resources.

Passwords offer the benefits of being relatively inexpensive, readily implementable and supported by most operating systems (Spender, 1987). A fourth benefit of adopting a password security system is familiarity. Passwords are a known methodology. They are viewed as a simple, friendly method to control access. Emphasis placed on ease of use may, unfortunately, hamper the degree of security provided.

C. TRADEOFF: EASE OF USE VERSUS SECURITY

Ease of use is defined as user-friendliness and flexibility (Wood, 1983). Some users have developed an attitude that it is their right to use computer resources as they desire, commonly known as the hacker ethic. Concurrent with this attitude is a desire by users to avoid any restrictions on their ability to gain access at any time and anywhere. The current proliferation of local area networks has greatly enhanced this desire to gain access at the office, at home or on the road. The widespread availability of personal computers connected to central databases has resulted in organizations granting access to more users. Paans and Herschberg (1987) note that there is a lack of enthusiasm among the lower ranks for security as they feel controls tend to degrade their happiness. If password and sign-on procedures becomes difficult, users will find ways to circumvent it, thereby degrading security (Martin, 1973).

The ease of use versus security tradeoff is directly applicable to passwords. Passwords must strike a balance between ease of remembrance by a user and difficulty of guessing by outsiders. The longer the password, the more difficult it is to guess (Wood, 1983). Unfortunately, most users require aids to help their recall (Menkus, 1988). If a password is so long that a user must write it down, security has been degraded. If a user puts a password on paper, it changes from something known to something possessed. Knowledge of the hiding place of the paper with the password written on it becomes the password (Porter, 1982). Figure 3-1 illustrates the tradeoff between ease of use and security.

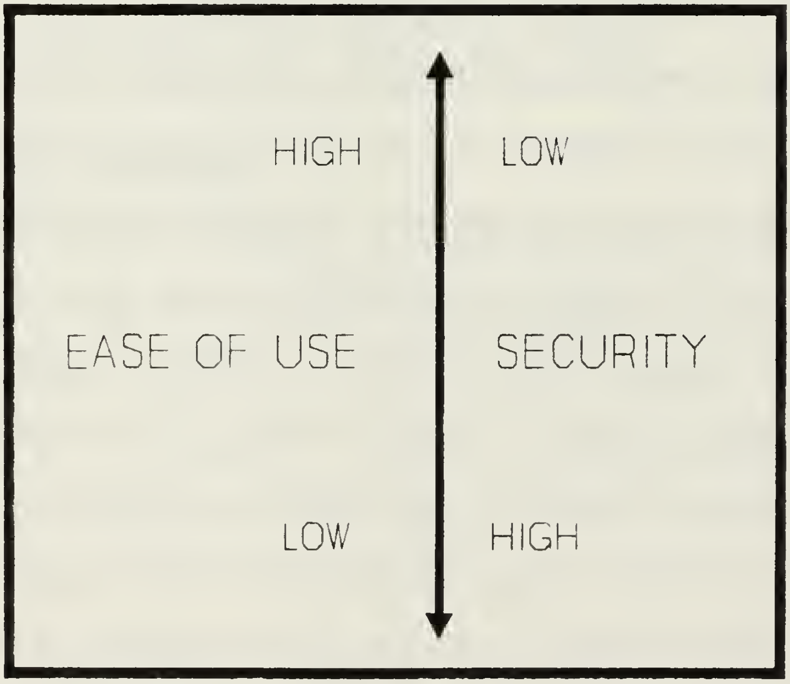

FIGURE 3-1
TRADEOFF: EASE OF USE VERSUS SECURITY

D. OBJECTIVES OF PASSWORDS

The objective of a password is to authenticate a user of computer resources (Wood, 1983). As the system authenticator, passwords are the first line of defense against unauthorized use of computer systems (Wood, 1983).

Protection of personal privacy, proprietary interests, administrative confidentiality (Barton, et al., 1984) and, in the military, national security might be achieved through passwords. The privacy of personal information such as social security numbers is a concern in large databases. The development of proprietary interests such as processes stored in computers must be protected from industrial espionage. Confidential records such as payroll records must be protected from intruders trying to change pay rates or create phantom employee records for embezzlement. Unauthorized access into military databases could result in being unprepared for an attack.

In achieving a level of protection from intruders, passwords can prevent, detect and deter (Wood, 1983). Passwords are the second layer of a computer security system. A determined intruder may not be deterred by a single layer of protection. Multilayered systems can make the time and effort necessary to break into the system so expensive that intruders will feel it is not cost effective. Passwords are used in an attempt to raise the cost of penetrating a system to a level where an intruder is either prevented or deterred (Wood, 1983). Menkus (1988) recommends optimizing password performance by making compromise as difficult and time consuming as possible. Monitoring programs can be added to password systems that track attempted accesses and alert system personnel.

E. TYPES OF PASSWORDS

Passwords are categorized by two methods: generation and use. Generation methods include system, user and manufacturer. Use methods include primary, secondary and dynamic.

1. System Generated Passwords

The system generation of passwords is managed by a system security administrator (Menkus, 1988). The administrator's responsibilities include selection of new passwords, distribution of passwords, monitoring to ensure proper use of passwords and disposition of expired passwords. System generated passwords are normally generated either through a random number generator or a nonsense string generator (Menkus, 1988).

The advantage of system generated passwords is that the user is removed from the selection process. User generated passwords are normally connected with the user's lifestyle and therefore are vulnerable to guessing by outsiders (Menkus, 1988). System generated passwords will normally contain random characters and are not related to a user's lifestyle.

Disadvantages of system generated passwords include difficulty in remembering, possible repetition of generation cycles, vulnerability of storage tables and the removal of the user from the selection process. Nonsensical strings of characters make guessing difficult, but also make remembrance by a user difficult. Complicated passwords tend to be forgotten or written down (Ahituv, et al., 1987).

To combat this problem, some systems generate character strings that include vowels, making the strings more pronounceable and therefore memorable. The tradeoff in making system generated passwords pronounceable is that the passwords are more vulnerable (Kurzban, 1983).

2. User Generated Passwords

User selected passwords tend to be simple and composed of birthday dates, spouse's names, nicknames and other data connected with a user's lifestyle (Menkus, 1988). In many cases, passwords can be found in personnel files. The Department of Defense forms teams of computer experts to test the integrity of security systems. These tiger teams routinely comb personnel files, for passwords based on personal data, with great success (Wood, 1983).

User selected passwords have the advantage of being simple and meaningful. The disadvantage is that they are frequently based on trivial association and can be guessed by outsiders (Ahituv, et al., 1987).

3. Manufacturer Generated Passwords

Manufacturers typically embed or hard-code passwords into programs. These embedded passwords serve as example passwords and are published in system documentation (Wood, 1983). Example passwords are intended to be temporary until the user selects a replacement. If the user does not remove the example password, it may become a source of vulnerability.

Another type of manufacturer's password is that used by field representatives and technicians. These passwords typically take the form of "test" and "system"

(Barton, et. al., 1984). They serve as a quick method by which technicians can gain access for maintenance and repairs. Knowledge of these passwords may allow unauthorized users to penetrate a security system.

4. Classification by Use

Passwords are also classified by their use: primary, secondary and dynamic. Primary passwords are used to gain access to an initial set of resources (Menkus, 1988). Secondary passwords are used as supplements to gain access to a subset of resources (Menkus, 1988). Dynamic use of passwords involves use of a different password at each log-in (Avarne, 1988).

F. EXTENDED PASSWORDS (PASSPHRASES)

Passwords, either system or user generated, share the problem of memorability. If users construct the password, it is easy to remember but unsecure (Wood, 1983). System generated passwords are secure but unpopular with users (Wood, 1983). The longer the password, the more secure it is (Menkus, 1988). However, the longer the password, the more complicated; users tend to forget long passwords or they write them down (Ahituv, et al., 1987).

In order to take advantage of the best of both the system and user generation methods, extended passwords or passphrases were developed as a compromise (Wood, 1983). Passphrases are long passwords normally consisting of thirty to eighty characters (Porter, 1982). Menkus (1988) describes an extended password as an easily remembered but nonsensical three or four word phrase. Passphrases offer the advantage

of allowing a user to select a password for himself. A passphrase is more likely to be meaningful and therefore easier for a user to remember (Porter, 1982). An additional advantage of extended passwords is the added length of the password. Passwords should be long enough that they will yield at least one million possible combinations (Fisher, 1984). Using a minimum of 30 alphabetic characters, over one trillion combinations are possible. This foils at least one way used to determine someone's password: trying all possible character combinations (Pfleeger, 1989). The sheer magnitude of the effort and time required by an intruder to perform an exhaustive search poses a high level of deterrence.

Additional schemes may be employed in conjunction with passphrases. A thirty to eighty character passphrase can be put through a hashing algorithm. Hashing extracts a number of designated characters from an extended password. Extracted characters constitute an actual password that is stored in an access table. Hashing a passphrase reduces the amount of required memory storage and provides one-way encryption (Porter, 1982).

G. CONSTRUCTION OF PASSWORDS

The success of passwords as a security mechanism is related directly to good construction. Three criteria govern good construction: length, character set and memorability.

1. Length

The longer the password, the more difficult it is to guess it and therefore the more secure it is (Wood, 1983). Passwords are commonly constructed of six to eight characters. This length is popular for two reasons: first, six to eight characters are sufficient to guard against a "brute-force" attack (Wood, 1983) and second, memory aids are commonly required for recall of passwords of more than eight characters (Menkus, 1988). The elimination of memory aids decreases the probability that passwords will be committed to paper.

The minimum length of a password determines the lower bound of security (Menkus, 1988). Fisher (1983) suggests that the minimum length should be a set of characters that would yield at least one million possible combinations. The following sets meet this minimum constraint: six decimal digits, e.g., 195863; five hexadecimal characters, e.g., 1D6FC; five alphabetic characters, e.g., AZHWO or four alphanumeric characters, e.g., HW39 (Fisher, 1984). A consideration in selecting a minimum length is that intruders will be attracted to trying all possible combinations; i.e., an exhaustive or brute-force attack. In an exhaustive attack, an intruder will have to try no more than forty per cent of the possibilities to break a password (Menkus, 1988). A password composed of three numeric characters yields one thousand possibilities. A computer programmed to try each of the possible combinations will likely break the password in little time. Doubling the length will increase the effort required by orders of magnitude (Menkus, 1988). If three numerics were increased to six numerics, the combinations increase from one thousand to one million.

The design of the length of passwords should also consider whether a system will allow a user to construct a password that is shorter than the maximum. For example, if a password is designed to be eight numeric characters, will a system allow a user to use only four characters? Most systems will enter trailing blanks in the unfilled spaces (Menkus, 1988). A common ploy is for the potential penetrator to concentrate on trailing blanks first (Menkus, 1988). The elimination of the blanks will significantly reduced the total combinations that the intruder must attempt. By eliminating four trailing blanks, an intruder reduces the work factor from one hundred million to ten thousand possibilities.

2. Character Set

The set of characters coupled with the number of characters determines the effectiveness of passwords. The ideal password is composed of random characters, such as "k&)8[" (Barton, et al., 1984). While random characters are more secure, they are seldom pronounceable. When a password is pronounceable, users will be better able to remember it (Kurzban, 1983). The addition of vowels increases pronounceability. However, the resulting password will be more vulnerable to attack (Kurzban, 1983). For example, if vowels are inserted into the string CTWLK, it becomes CATWALK.

3. Memorability

The ability to remember and recall passwords is of paramount importance in their construction. Most users require memory aids to help recall (Menkus, 1988). If a memory aid means writing the password on paper, a basic tenet of password

security has been violated. A password committed to paper has changed from something known to something possessed (Porter, 1984). An intruder's work switches from guessing to searching.

An appeal to long term memory has been divided into two classifications of memory: semantic and episodic. These two classes form the basis for three approaches to enhancing the memorability of passwords: semantic, episodic and environmental (Barton, et al., 1984).

a. Semantic

Semantic memory uses information closely related to language use. Passwords using this approach are derived from well-known character strings, such as nursery rhymes. Nursery rhymes and similar strings are easily recalled, thereby eliminating the need for memory aids. For example, "Jack and Jill went up the hill" is a well known line from a childhood poem. In addition, these character strings are not related to a user's lifestyle. Once identified, the string can be used with a hashing routine or a transform procedure to produce a phoneme, word or phrase that is actually the password.

b. Episodic

Episodic memory relies directly on individual, personal experience. To a large degree, this experience will be unshared. Provided the user avoids the obvious references to experience, such as birthday dates and children's names, this type of memory is recommended for password systems. Transform procedures can operate in conjunction with episodic memory to produce passwords.

c. *Environmental*

Environmental clues trigger the recall of passwords. A picture on the office wall or a room number can serve as the basis of a character string. If the user's terminal is located in a room that is painted green, "green walls" could serve as the initial character string. If a user's office is in room 821 at 1275 Sams Street, 8211275 could serve as the environmental trigger for a password. This string could then be manipulated by a transform procedure to produce the actual password. In the above example of 8211275, a transform procedure could take the even digits of 822 and add that result back to the initial room number to come up with the final password; i.e., 822 plus 821 equals 1643. In this example, 1643 is the password triggered by the environmental clue of the room number 821.

4. Transform Procedures

Character strings produced by any of the three methods above can be coupled with transform procedures. A transform procedure manipulates a string to produce a user- recognizable and memorable password (Barton, et al., 1984). Effective transform procedures are evaluated on the following criteria: ability to achieve a high degree of congeniality; i.e., easy to remember and to execute; ability to produce structured passwords that can be recreated which helps error discovery and ability to produce passwords resistant to guessing and systematic trials. Common transform techniques are excerption and substitution. In excerption, a designated number of characters are excerpted based on their position within a string. The excerpted

characters form the actual password. Substitution can also be used. Common substitution practices include the substitution of preceding or succeeding characters. The resulting string of substituted characters constitutes the password. (Barton, et al., 1984)

5. Mnemonics

Closely related to transform procedures are mnemonics. The phonetic sounding of a character string may yield an expression that is pronounceable and memorable (Barton, et al., 1984). For example, the character string FRGTFL could be phonetically sounded as FOR-GET-FUL. While FRGTFL is the password, the phrase FOR-GET-FUL is the mnemonic that causes the password to be memorable. Other ways of avoiding memory aids are: inverting the order of characters, converting alphabetic characters to their numeric equivalents, shifting characters one or two positions and creating acronyms from initial letters of a meaningful phrase (Menkus, 1988).

6. Summary

Good formulation produces passwords that are distanced enough in form from ordinary experience to make compromise unlikely (Barton, et al., 1984). Whether produced by semantic, episodic or environmental methodologies, passwords should be evaluated for effectiveness. Ahituv, Lapid and Neumann (1987) propose the following evaluation criteria:

1. should be easily memorized,
2. should be hard to guess through association,

3. should be easy to enter into the computer,

4. should not be able to be used if expired,

5. should be resistant to attack by spoofing or trojan horses,

6. should be tested,

7. should not take a long time to implement and

8. should not be cost prohibitive.

H. PROBLEMS WITH PASSWORDS

The use of passwords as a security mechanism is a much debated topic. Opinions on effectiveness range from criticism as offering little resistance to a serious attack (Avarne, 1988) and their use is rarely well managed (Menkus, 1988) to praise as the most cost-effective approach to human user authentication (Wood, 1983). Menkus (1988) makes the comparison of a password to a conventional lock; it keeps out only honest people.

Traditional passwords have three weaknesses: they can often be guessed, they are entered in the clear where they can be observed and they are used more than once (Avarne, 1988). These weaknesses are further supplemented by Ahituv, Lapid and Neumann (1987): passwords are normally stored in tables in an operating system which itself is subject to compromise and spoof routines. Spoof routines, explained below, can be used during a log-in procedure to capture passwords from an unsuspecting user.

Eight methods of finding out a password have been identified: guessing, reading, hash tables, eavesdropping, intercept, signal radiation, spoofing and terminal buffers (Avarne, 1988).

1. Guessing

Users commonly use names, telephone numbers and other trivial but memorable data as passwords. Guessing entails repeated trials based on a certain amount of knowledge. To prevent guessing, systems may be equipped with counter programs that allow only a certain number of unsuccessful attempts before freezing out a would-be user. Such systems can still be penetrated through the intruder attempting one less than the maximum allowable attempts each day until successful.

2. Reading

Passwords committed to paper are usually looked up just before a log-in. People nearby may see the location of a written password. Systems requiring frequent changes of passwords may increase the likelihood of users writing them down. In addition, frequent changes in passwords may be circumvented by re-entering an identical password or alternating between two passwords.

3. Hash Tables

Hash tables may lead to a false sense of security. An intruder needs only to know a hashed result of a password. Any character string that yields the same hashed result will suffice.

4. Eavesdropping

Most computer terminals do not echo a password back to the screen. Nonetheless, a person nearby may observe a sequence of keystrokes. Even listening to the number of keystrokes yields the length of a password.

5. Intercept

The proliferation of networks is a rich area for exploitation. Tapping into a line between a terminal and a host can give direct access to an intruder.

6. Signal Radiation

All electronic equipment, unless Tempest certified, emit radiomagnetic signals. These signals can be monitored and intercepted. Each keystroke emits a unique signal that can be correlated to give a direct interception of transmissions.

7. Spoofing

Penetrators develop programs that emulate terminal log-in procedures. A valid user enters a password not knowing that a spoof program is receiving the data instead of the computer. At the end of a log-in procedure, the computer gives an error message. The user assumes that a error has been made in keying in the information and re-enters the password. On the second try, the log-in is successful. Unbeknownst to an authorized user, an intruder now has a valid password and can enter the system at will.

8. Terminal Buffers

Passwords are written into a buffer from which the security program can read the entry. If a buffer is of large size or if system usage is low, a password may stay resident in a buffer for an indefinite time. An intruder monitoring a buffer may be able to read its passwords that are still resident.

I. MYTHS ABOUT PASSWORDS

Closely related to the problems associated with passwords are the unrealistic expectations of security provided by passwords. Of a list of twelve misconceptions about information processing security, four are relevant to passwords (Kurzban, 1983).

1. Pronounceability

Myth: If system generated passwords are pronounceable, users will remember them. The addition of vowels to nonsense strings may result in pronounceability, but they also make the password more vulnerable. Meaning acts as a natural memory aid. Kurzban recommends choosing passwords that are hard to guess, not hard to remember.

2. Incorrect Passwords

Myth: An incorrect password indicates an attempt to gain unauthorized access. Most incorrect passwords are from authorized users who have either forgotten or miskeyed. The owner has lost the password and tries to guess it through trial and error (Panns, et al., 1987).

3. Revoking Rights

Myth: Successive incorrect passwords indicate an unauthorized user and the rights of the password owner should be revoked. As in Myth 2, most incorrect passwords result from legitimate users. An intruder can sabotage a system by entering successive passwords that result in the valid user being frozen out of the system. Without actually breaking into the computer system, the potential intruder has significantly affected both the users and the system.

4. Layered Passwords

Myth: A different password for each resource layer enhances security. While a certain benefit may be gained from layered passwords, users resent multiple passwords and may seek revenge on the system.

J. ADMINISTRATION OF PASSWORDS

Password systems require maintenance. Akin to logical fences, passwords systems require periodic maintenance (Wood, 1983). In large systems, security may be in the hands of a full-time security manager. In smaller systems, security is likely to be part of a system administrator's job.

A security manager is responsible for maintaining and modifying a computer system's security. As well as duties related to passwords, a manager is responsible for physical security and disaster recovery. Monitoring a system for evidence of tampering and proper password use are a security manager's primary duties.

User education in security matters is also a concern of a security manager (Wood, 1983). Users have certain responsibilities when using the system and should be duly aware of the consequences of inappropriate actions (Panns, et al., 1987). Education will make users aware of how a password system can protect their information from unauthorized access. At the same time, educated users will be aware of how the design and protection of passwords can enhance overall system security. Help with developing passwords should be available on-line. Technical information about length, type of characters and ranges should be accessible to users (Barton, et al., 1984).

K. PASSWORD SYSTEM IMPLEMENTATION

Wood (1983) asserts that a password security system is successful if it meets the following criteria:

1. Passwords are not visible when typed.
2. An alarm is generated if successive log-in attempts exceed a specified threshold.
3. A password storage table is encrypted and is not reversible.
4. Passwords travelling over networks are encrypted.
5. Provision is made for a special password to indicate a user is under duress and is being forced to log-in.
6. Error messages are limited to a single message that does not indicate which step in the log-in process was wrong.
7. A password routine is segregated from the resource that it protects.
8. Re-verification of a password is required if a session exceeds a specified time limit.

9. Automatic log-off occurs if no activity takes place after a prescribed time period.

Successful implementation of system-generated passwords should include provisions for the secure distribution of passwords. Two common distribution methods are (1) conventional mail using double envelopes or specially designed envelopes that mask a password and (2) network transmission using encryption (Menkus, 1988). A user-selected password system eliminates the need for a password distribution system (Spender, 1987).

A password security system requires the commitment of top management. Information is a strategic resource. Lost or damaged information may have costly implications for an organization. Historically, hardware was the major cost of a computer system. In recent information systems, software is the major expense. Management often uses hardware values instead of the value of the information to base their security decisions (Wood, 1983).

Menkus (1988) identifies five ways to improve performance of a password security system:

1. insist that an organization's policies are enforced,
2. prohibit storing of passwords in tables to speed network connectivity,
3. penalize deliberate disclosure of passwords no matter how good an excuse,
4. require frequent password-changing and
5. insist that passwords be actually changed.

L. PROTECTION OF PASSWORDS

Successfully breaking a password may allow an unauthorized user total access to a computer system. In many systems, passwords are not only the first line of defense (Wood, 1983) they are the only line of defense. With the importance placed on passwords, security of passwords is a major concern. Passwords may be compromised by:

1. trying all possibilities;
2. trying all probable passwords;
3. trying passwords likely for a user;
4. searching for a system list of passwords;
5. asking a user. (Pfleeger, 1989)

Additional protection may be had through the use of encryption. Techniques include encryption of password tables stored in memory, use of one-time encrypted passwords and use of personal keys that are inserted after a plain text password is entered (Ahituv, et al., 1987). One-way encryption increases the work needed to enter a system (Menkus, 1988). Encryption of password tables may be accomplished by the simple addition or subtraction of some constant (Menkus, 1988). Whichever encryption method is used, care should be given to ensure that an encryption process does not expose encryption techniques used for other resources (Ahituv, et al., 1987).

M. SUMMARY

Passwords can be an inexpensive, effective means to system security. The tradeoff between memorability (ease of use) and security will affect a user's environment. If a user's environment is unfriendly, a user will find ways of overcoming the difficulty and in turn, may compromise system security (Martin, 1973). A hostile environment is caused by an emphasis on security at the expense of password memorability (Barton, et al., 1984).

IV. NEW APPROACHES TO PASSWORDS

A. IS THERE A BETTER WAY?

Traditional passwords have advantages and disadvantages. Inexpensive, readily implemented and supported by most operating systems (Spender, 1987) are the advantages of passwords. The need for memory aids and potentially hostile environments are among their disadvantages. Opinions about the effectiveness of passwords range from seeing them as useless against attack (Avarne, 1988) to calling them the most cost-effective approach to human user authentication (Wood, 1983).

Balanced between these views are the issues of memorability and security (Barton, et al., 1984). Smith (1987) recommends that systems be made easier to use and harder to misuse. The crux of the problem is to develop a fast, reliable identification process that will not hinder users or effective computer use (Smith, 1987).

The perceived inability of traditional passwords to support adequate levels of security plus demands from users for a friendly environment have lead to several new approaches. Identity-authentication can be accomplished in four ways:

1. something possessed (Porter, 1982),
2. something characteristic of a user (Porter, 1982),
3. something known (Porter, 1982),
4. something the user can do (Spender, 1987).

1. Something Possessed

Identification of users by possession of a physical object has gained popularity. The advent of banking system automatic teller machine systems has led millions of people to become familiar with physical tokens, such as bank authentication cards. Most automatic teller systems are coupled with a secondary identification process: a personal identification number must be keyed into the system to gain access. Authentication by something possessed coupled with something known (Wood, 1983) has been very successful. Identification by possession is not secure. Tokens can be lost, stolen or copied (Smith, 1987).

2. Something Characteristic of a User

Biometric authentication using natural properties of a user, such as fingerprints, is an emerging technology (Ahituv, et al., 1987). A drawback of biometrics is the requirement of special equipment to recognize and transmit the property. Two methods of breaking the biometric system are (1) faking the pattern that corresponds to the digital representation of the trait or occurrence and (2) modifying the table that stores the trait representations (Ahituv, et al., 1987).

3. Something Known

Passwords, something known, even with the previously described faults, are an economical, viable security mechanism. A common reaction to password problems is the imposition of constraints. While well intentioned, many of these constraints have only exacerbated the problem. Ineffective efforts to make passwords more secure will also make authentication more difficult (Smith, 1987). The U.S. Department of

Defense recommends that user-generated passwords be replaced by system-generated passwords (CSC-STD-002-85, 1985). Complicated passwords tend to be forgotten and are written down (Ahituv, et al., 1987).

4. Something a User Can Do

Closely related to the category of something characteristic of a user is identification based on something the user can do, such as write a signature (Spender, 1987). Identification based on the user's ability to perform a specific action has advantages and disadvantages similar to authentication based on a user's characteristics: both require special equipment in order to read and interpret the occurrence. Both systems may be defeated by either knowing the interpreted results of the mechanism or gain access to the table containing the occurrence representations (Ahituv, et al., 1987).

B. NEW APPROACHES

Smith (1987) suggests three new and creative approaches to password authentication systems: a biographical model, a personal interests model and a word association model.

1. Biographical Model

This model is based on biographical data that would normally not be available to an intruder. For example, a user's mother's maiden name or the first name of a user's first girlfriend or boyfriend could be used to develop a password. Screening of data would ensure that the biographical data could not be found in

personnel records. In the above examples, both answers are seldom in personnel records and are usually known only by the specific user. Smith postulates one problem: users might resent being asked to divulge such information.

2. Personal Interest Model

The personal interest model is based on a dialogue between a user and a computer by which a computer can assess the validity of an identity claim. A user's habits or opinions can form the basis for development of a password. For example, a user's favorite color or a user's favorite dessert may serve as the basis of a password. Advantages of these two examples are that both answers are not normally found in personnel records and are usually known only by the user. Drawbacks of the personal interest model are the length of a dialogue session and user resistance to the questions.

3. Word Association Model

Smith (1987) proposes a system identification test based on the following criteria:

1. quick identification of users through individualistic responses;
2. entails little recall burden; i.e., information should have a high degree of congeniality;
3. the process should be designed to minimize user resentment.

Using these criteria, Smith proposed a password system based on word association. Examples of such associations might be the cue "officer" followed by the response of "Navy". Four advantages were postulated:

1. reliable identification through uniqueness to an individual,
2. robustness and resistance to intrusion,
3. high memorability and
4. little user resistance by allowing a user to select paired words. (Smith, 1987)

Smith designed his word association model using two criteria: structure and memorability.

a. Structure

The system would be implemented by having a user enter a list of twenty words as cues. Cues and responses are user selected. Single words were selected to ensure higher recall and ease of entry. At an initial session, a user enters the paired responses. At a subsequent session, a user is prompted by a randomly selected cue. In return, an associated response is entered. If a cue and a response match, access is granted. As long as stereotype associations such as "blue-sky" are avoided, each cue and response is unique to the user and therefore harder to break.

b. Memorability

A primary concern was the ability of a user to recall responses over an extended time. A group of users were selected as the test population. In a test six months after the initial administration, users were asked to recall cues and responses. Recall averaged twenty-four per cent for cues and ninety four per cent for responses. Eighteen months after the initial administration. the members were again tested. Recall averaged twenty nine per cent for cues and eighty six per cent for responses. Unfortunately a sample of only four users was used in this test. Nonetheless, the point

is that cues can serve as memory aids. Users need memory aids to recall passwords (Menkus, 1988). User selected passwords are easier to remember (Wood, 1983). Being user-selected, responses reflect personal associations. Personal association is based on episodic memory which is preferred for password formulation (Barton, et al., 1984).

c. Vulnerability to Attack

Attack by trying all possible combinations is defeated by the sheer magnitude of the required effort. In order to successfully break a word association, an intruder must know both a cue and its paired response. A cue and response could be structured to consist of a minimum of three alphabetic characters and a maximum of eight alphabetic characters. This structure yields a minimum of three million possible passwords and a maximum of two billion. Without contextual knowledge of word pairs, intruders would have little chance of breaking such a system (Smith, 1987). Paired cues and responses are stored in tables in memory. The table is encrypted to reduce its chance of compromise. However, a word association model suffers the same problems as other password systems: interception, eavesdropping and monitoring (Smith, 1987).

d. Conclusions

Smith (1987) found the word association model to be robust and offered the following advantages:

1. users do not need to remember cues,
2. users do not need a printed cue list as a memory aid,

3. users do not need to display their entire paired cue response list unless conducting periodic changes and

4. users do not need the response echoed to the terminal screen.

e. Summary

The Smith Word Association Model highlights how traditional password systems can be improved to make them more robust and less vulnerable to attack. One of the most common complaints concerning passwords is that they offer little resistance to a serious attack (Avarne, 1988). The magnitude of the time and effort required to break this system is so great that it acts as an effective deterrent to even the most serious attacker. Figure 4-1 evaluates the word association model based on Ahituv, Lapid and Neumann's (1984) criteria described in Chapter III.

EVALUATION OF THE
WORD ASSOCIATION MODEL

CRITERIA	MODEL
1. EASILY REMEMBERED ?	YES
2. HARD TO GUESS BY ASSOCIATION ?	YES
3 EASY TO KEY-IN ?	YES
4 ATTACKABLE BY SPOOFING OR TROJAN HORSE ?	YES
5 TESTED ?	YES
6 EASY TO IMPLEMENT ?	YES
7 COST PROHIBITIVE ?	NO

FIGURE 4-1

4. Cognitive Password Model

An outgrowth of Smith's (1987) three models is a cognitive password model, the main subject of this paper. A cognitive password system uses passwords based on perception, intuition, personal interests and personal history; i.e., Smith's (1987) biographical and personal interest models.

a. *Advantages of Cognitive Passwords*

A biographical model offers the advantage of information not normally found in personnel records (Smith, 1987). This information is known only to the user, thereby making guessing difficult. A personal interest model affords the advantage of easy recall without a need for memory aids (Smith, 1987). Since the information is significant to the user, he or she is able to remember without a memory aid, thereby eliminating the possibility of a password being changed from something known to something possessed.

Since both biographical and personal interest models are used, the advantages of each model accrue to a cognitive system. A cognitive password system is based on information not normally found in personnel records, on personal information and on information that is easily recalled.

b. *Ease of Use versus Security Tradeoff*

The tradeoff between ease of use and security is a major concern of security managers (Wood, 1983). The easier a password is to use or remember, the less security it offers, normally through requiring a memory aid (Wood, 1983). Similarly, the more security a password offers, the harder it is to use or remember (Ahituv, et al., 1987). Figure 3-1 in Chapter III illustrates this tradeoff. A cognitive password system resolves this dilemma to a greater degree than does traditional passwords. A cognitive password is composed of significant events, biographical data, personal habits or personal interests. As the selected information is significant and personal to the user, he or she is able to recall the information without the need for

a memory aid, thereby satisfying the ease of use requirement. The degree of security provided by a password is based on two criteria: need for memory aids and ability to be guessed. The elimination of the need for a memory aid has already been discussed. Guessing is a primary method of password compromise (Avarne, 1988). Guessing can be accomplished through trivial association, such as a spouse's name and birthday dates (Ahituv, et al., 1987). A cognitive password system defeats guessing since cognitive passwords are based on information not easily associated with the user.

c. User-related versus System-generated

Traditional passwords are developed in two ways: user-selected or system-generated. User-selected passwords tend to be simple (Menkus, 1988) and are based on trivial association, such as a spouse's name (Ahituv, et al., 1987). While easily recalled, user-selected passwords are easily guessed and therefore afford a low degree of security (Ahituv, et al., 1987). System-generated passwords are strings of nonsensical characters (Menkus, 1988). A nonsensical string makes guessing harder, but it makes remembrance more difficult, thereby requiring memory aids (Ahituv, et al., 1987). Cognitive passwords combine the advantages of both types of traditional passwords. A user selects a cognitive password based on personal, non-trivial information. Since the password is based on significant information, recall is high without the need for memory aids. At the same time, since a selected password is not easily guessed, it provides a higher degree of security than traditional passwords.

d. Construction

Success of password systems is directly related to good construction. Cognitive passwords satisfies the three elements of good construction: length, character set and memorability.

(1) Length. The minimum number of characters comprising a password sets the lower security bound (Menkus, 1988). A threshold of 1,000,000 possible combinations is adequate for most systems (Fisher, 1983). A common length is six to eight characters (Wood, 1983). This length is sufficient to deter "brute-force" attacks (Wood, 1983) and memory aids are not normally required (Menkus, 1988). The implemented cognitive password model is comprised of twenty passwords of a maximum of twenty characters each. While not all twenty sets of passwords questions and answers are required to gain access, an intruder must know all twenty answers in order to ensure entry. A minimum length is not specified, but a minimum of five to six characters per answer is anticipated. Assuming a minimum average of five alphabetic characters, each set has over 11,000,000 possible combinations. The cognitive authentication process allows a maximum of ten questions per session for a total of 110,000,000 possible combinations. Any "brute-force" attack will require considerable time and effort, thereby either preventing or deterring an attacker (Wood, 1983).

(2) Character Set. Pronounceability, the addition of vowels to characters, is a major issue in password construction. Random characters yield the highest degree of security (Barton, et al., 1984), but they are neither pronounceable, nor memorable (Kurzban, 1983). If passwords are pronounceable, they are more vulnerable to attack (Kurzban, 1983). Cognitive passwords offer the advantage of pronounceability plus they are less vulnerable to attack. A user selects meaningful answers to cognitive password questions. These answers are pronounceable, but since they are not readily associated with the user, the answers are less vulnerable to attack.

(3) Memorability. The degree of memorability determines the need for memory aids. Elimination of the need for memory aids protect passwords from being changed from something known to something possessed (Porter, 1984). Of the two types of long term memory, semantic and episodic, episodic memory is recommended for password use (Barton, et al., 1984). Episodic memory is based on individual and unshared personal experience (Barton, 1984). Cognitive passwords offer the advantages of not requiring memory aids and being based on episodic memory.

e. Summary

A cognitive password security system surpasses traditional password systems in the areas of ease of use versus security, user-selected versus system-generated and construction. Chapters V and VI cover research into the memorability of cognitive versus traditional passwords. Chapter VII explores a prototype of a cognitive password system.

V. RESEARCH METHODOLOGY

A. BACKGROUND

A basic premise of the cognitive password system is that the users provide the data upon which the cognitive password challenges are based. This data consists of three types: fact-based, interest-based and opinion-based that is normally known only to the user. A fact-based challenge asks something that a user knows but is a fact independent of a user's regard, e.g., "What is the name of the elementary school that you last attended?" An interest-based item might ask "What is your favorite type of music?" An example of an opinion-based question would be "What is you favorite flower?"

Of crucial interest in this research is the memorability of cognitive passwords and their susceptibility to guessing by people closely associated with the users. A simultaneous test of the recall of system-generated passwords (random alphanumeric seven-character strings) and user-created passwords is conducted. If cognitive passwords can be shown to possess both a high degree of memorability and low degree of vulnerability to guessing, the cognitive password system can be shown to be based on a robust foundation that yields high ease of use and a high degree of security.

B. METHODOLOGY

The following is a description of the methodology used in gathering data for this paper.

1. Instrumentation

To assess the ease of recall for cognitive passwords, three forms of similar self-administered questionnaires were developed. A copy of each questionnaire form is included in the appendix. Each user-respondent answered the first and third forms of the questionnaire, Q1 and Q2. They were answered by the primary respondents in the study which were designated variously as the user-respondents or the Q1 respondents. A significant-other (spouse, close friend or sibling) for each user-respondent completed the second form. This questionnaire was designated the Q2 form.

a. Demographic Items

Both the Q1 and Q3 forms asked for three categories of responses. The first part of Q1 asked for the respondent's age, sex, years of computer usage, types of computer with which they were experienced (mainframe terminal, stand-alone micro or micro linked to mainframe) and the last four digits of the respondent's Social Security number. The Q3 form asked only for the Social Security number digits, so that it could be matched with its Q1 counterpart. The Social Security digits are used to mask the identity of individual respondents in the data base of this study, while allowing matching of the Q1, Q2 and Q3 forms during the course of the research.

b. *Creation and Assignment of Passwords*

The second part of Q1, but not Q3, asked each respondent to create a password consisting of any combination of up to eight alphanumeric characters. The test group was urged to memorize and safeguard this password as they would any other password. They were then asked how they devised this password. Four choices were given: (1) does the password represent a meaningful detail such as a name, a date or a number; (2) does the password represent a combination of meaningful details; (3) does the password represent a random choice of characters or (4) other. The second part of Q1 displayed a unique seven-character password that was assigned to each respondent. The password was constructed of a random combination of letters and numbers. The respondents were urged to memorize and safeguard this password as well.

c. *Cognitive Data Items*

The Q1 and Q3 forms are identical in their third section. In this part, 20 open response items ask for items of information that were described as cognitive data. These data fall into two categories of responses. In the first group, six items ask for personal facts that were assumed that only a respondent or someone socially close to a respondent would know. For example: elementary school attended, first name of favorite uncle, first name of best friend in high school, mother's maiden name, first name of first boyfriend/girlfriend and father's occupation. In the second group, 14 interest-based and opinion-based items ask each respondent to declare a favorite. For example: favorite music, favorite color, favorite flower, favorite vegetable and

favorite dessert. Again, the assumption was made that these responses would be known only by a respondent or by someone close to him or her.

d. *Items for Recall of Cognitive Data*

In the identical Q3 version of the cognitive data section, the same respondents were asked the same questions again approximately three months from the first administration. In examining the feasibility of a system of passwords based upon cognitive data, the correlation of responses between the Q1 and Q3 administrations is of interest. Expectations are that there will be a high correlation between the six fact-based cognitive items. Also of interest is to what extent the opinion-based cognitive data "favorites" might vary with the passage of time.

e. *Items for Recall of Passwords*

Where Q1 assigned a random password and asked for the creation of a password, the second part of Q3 asked the same respondents, at a later time, to recall these passwords. First after asking each person to recall the password of his or her own making, each respondent was asked whether he recalled his password from memory or had resorted to writing it down. Secondly, each respondent was asked to recall the assigned password on the Q1 form. The respondents were again asked whether they recalled it from memory or had written it down. Expectations were that the respondents would recall the passwords they created better than the assigned random string of characters. Additionally, of interest was the extent to which the use of a written memory aid confounded that expectation.

f. Items to Tap Socially-Close Knowledge of Cognitive Data

The Q2 significant-other form asked for only two items of identifying data. It asked for the last four digits of the user-respondent's Social Security number to be used for matching purposes. It then asked for the relationship of the Q2 significant-other respondent to the Q1 respondent. The remainder of the Q2 form repeated the 20 cognitive data items in the third section of the Q1 form. The significant-other respondent was asked to indicate what he or she thought the Q1 respondent would answer to each of the questions. They were asked to complete the Q2 form without help from the Q1 respondent. The Q2 respondents were also asked to answer only those items in which they were confident of their responses while leaving blank those where they would need to guess at the response. Of interest was the level of accuracy at which the Q2 significant-others could match the responses of the Q1 user-respondents. The assumption was that if someone socially-close to a user had deficient knowledge of personal cognitive data, then the likelihood of guessing by someone socially-distant from the same user would be remote.

2. Sample and Data Collection Design

a. Q1 Response by User-Respondent

The Q1 questionnaire was administered to 106 graduate students majoring in management information systems. The average age of the participants was 31.8 years in a range from 25 to 41 years. Of the respondents, 76% were male and 24% were female. They averaged four years of experience in using computers. All of the respondents had some experience with computers; the average was 4 years and

9.4% had been using them for less than a year. Forty five percent reported that they used some combination of microcomputer and mainframe, 30% said their computer experience was limited to microcomputers, while 12% claimed to use only a mainframe.

b. *Q2 Response by Significant-Other*

After completing Q1 forms, the user-respondents were given the Q2 form. They were asked to write the last four digits of their Social Security number on the form and then give it to a significant-other of their choosing. They were asked to return the Q2 forms within one week. Q2 forms were returned by 88 or 83% of the user-respondents. Of these, seven contained missing data, yielding 81 or 76% complete Q2 forms. Of the significant-others responding, 75% were spouses, 20% were friends and 5% were siblings.

c. *Q3 Response by User-Respondent*

The Q3 version of the questionnaire was administered to the same user-respondents approximately three months after the Q1 administration. Again, the administration was to the same test group that had completed Q1 forms. Of the original 106 Q1 respondents, 99 or 93% participated in the Q3 administration.

C. TABULATION

Upon completion of the administration of the Q1, Q2 and Q3 questionnaires, the data was tabulated and analized using standard statistical methods. Chapter VI explores the findings and results from the questionnaires.

VI. DATA ANALYSIS

A. FINDINGS

1. Recall of Passwords

Table 1 reflects the ability of the user-respondents to recall both the assigned password and the self-selected password. Of the user-respondents, 35.4% were able to accurately recall the password which they had created themselves three months earlier. Slightly over 23% of these user-respondents were able to recall the assigned seven-character random string password. Fourteen people accurately recalled both their self-generated password and the assigned password.

CONVENTIONAL PASSWORD RECALL

TYPE OF PASSWORD	NUMBER WHO RECALLED	PERCENT WHO RECALLED
Self-generated	35	35.4
Assigned	23	23.2

TABLE 1

The password recall results immediately provoke the question as to how the user-respondents were able to reproduce either of the two passwords three months later. Table 2 shows that 86% of the user-respondents reported that they recalled their self-generated password from memory without writing it down. The remaining 14% reported that they wrote down their self-generated passwords.

METHOD OF
CONVENTIONAL PASSWORD RECALL

METHOD OF RECALL	SELF-GENERATED	TYPE OF PASSWORD ASSIGNED
From memory	86%	34%
Written down	14%	66%
Total	100%	100%

TABLE 2

The expected opposite effect is found in the case of the assigned random-string password. When this password was assigned on the Q1 form, the likely response may have been that it was nonsensical and lacked any mnemonic character. This may have been motive enough for the user-respondents to write it down as, indeed, 65.8% of them did. Nonetheless, using a password of their own making and being confident that they would not need to write it down, only 35.4% of the

respondents could recall it three months later. Even where the user-respondents were sure they had to write it down, as in the case of the difficult-to-memorize assigned password, only 23.2% could recall it by the time of the Q3 administration. Apparently, people who could not recall their passwords also could not recall where they have written them down.

A meaningful detail was described to the respondents on the Q1 form of the questionnaire as an item such as a name, a date or a number. Table 3 shows that a overwhelming proportion, 77.2%, used some form of meaningful detail to create their own passwords.

METHODS OF
CREATING SELF-GENERATED PASSWORDS

METHOD	NUMBER	PERCENT
Meaningful detail	49	46.7
Combination of meaningful details	32	30.5
Random characters	8	7.6
Other	16	15.2

TABLE 3

2. Recall of Cognitive Data by User Respondents

The overall average number of correct matches by the user-respondents on all cognitive data questions between Q1 and Q3 was 16.3 out of 20 questions or 82%. Figure 6-1 reflects this distribution. Of interest is the congregation of the success rate of these user-respondents at the high end of the spectrum. While somewhat skewed, the distribution approximates that of a normal curve. The lowest level of success was 13 correct matches (65%) of cognitive data items out of a possible 20. The modal range is 15 to 17 correct responses (75% to 85%). Of interest is the comparison of the level of these responses on cognitive data with the responses for the two types of passwords recalled over the same period. The best password response was 35.2% for the self-generated passwords. On the cognitive data continuum, the number of correct matches for self-generated passwords would be equivalent to obtaining only seven correct cognitive matches. No respondent scored that poorly on cognitive data.

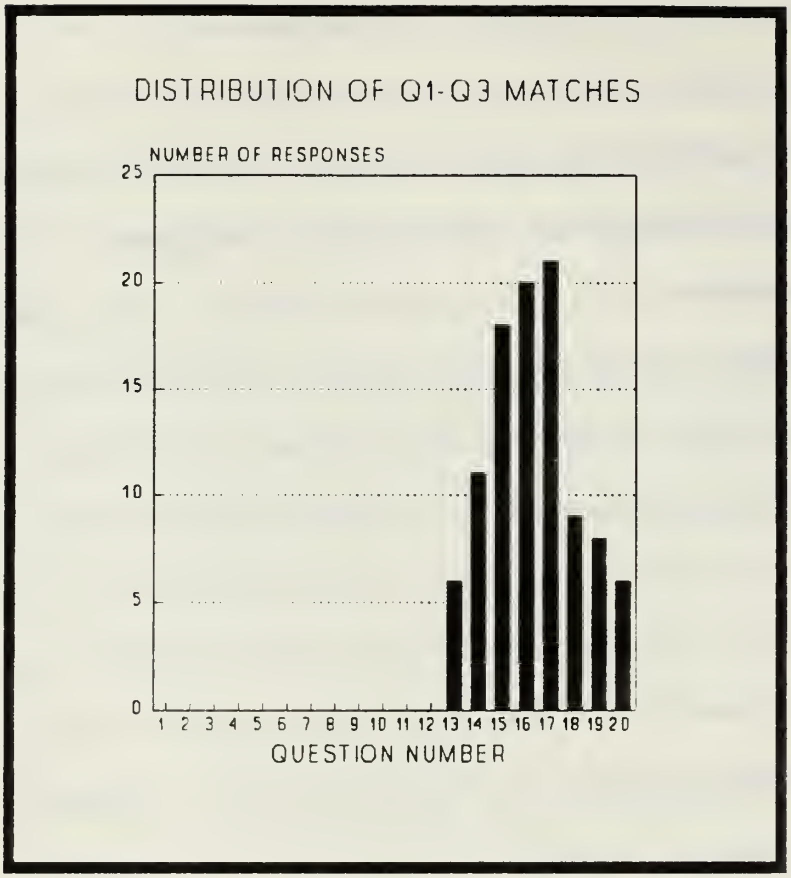

FIGURE 6-1

The success of these user-respondents in recalling cognitive data items over a three-month period is expressed in the percentage of correct matches that were produced on the Q3 form. The average for the fact-based cognitive items was 94.1% (Table 4). Only one of the responses was below 90%. Again, recall of self-generated passwords was 32.2%.

USER-RESPONDENT MATCHING ON
FACT-BASED COGNITIVE DATA ITEMS

ITEM	NUMBER WHO MATCHED CORRECTLY	PERCENT WHO MATCHED CORRECTLY
What is the name of the elementary school from which you graduated ?	93	93.9
What is the name of your favorite uncle ?	88	88.9
What is the name of your best friend in high school ?	9	9.9
What is your mother's maiden name ?	96	97.0
What was the first name of your first boyfriend or girlfriend ?	94	94.9
What is the occupation of your father ?	98	99.0

TABLE 4

As expected, the success rate for recall of the interest-based and opinion-based cognitive items is somewhat lower than that for the fact-based items. Nonetheless, the average percentage of correct responses produced on the Q3 form was 87.9%. The matches on a third of these items was over 90%. Only one item had a match rate below 80%. Tables 5, 6 and 7 portray the matching for interest and fact-based cognitive data items.

USER-RESPONDENT MATCHING ON INTEREST-BASED AND OPINION-BASED COGNITIVE DATA ITEMS

ITEM	NUMBER WHO MATCHED CORRECTLY	PERCENT WHO MATCHED CORRECTLY
What was the name of your favorite class in high school ?	80	80.8
What is the name of your favorite music performer or group ?	74	74.7
What is your favorite type of music ?	86	86.9
What is the name of your favorite vacation place ?	84	84.8
If you could travel to any country in the world, which would it be ?	85	85.9

TABLE 5

USER-RESPONDENT MATCHING ON INTEREST-BASED AND OPINION-BASED COGNITIVE DATA ITEMS

ITEM	NUMBER WHO MATCHED CORRECTLY	PERCENT WHO MATCHED CORRECTLY
What is the last name of your favorite actor or actress ?	83	83.8
What is your favorite flower ?	94	94.9
What is your favorite dessert ?	90	90.0
What is your favorite vegetable ?	85	85.9
What is your favorite fruit ?	86	86.9
What is your favorite color ?	95	96.0

TABLE 6

USER-RESPONDENT MATCHING ON INTEREST-BASED AND OPINION-BASED COGNITIVE DATA ITEMS

ITEM	NUMBER WHO MATCHED CORRECTLY	PERCENT WHO MATCHED CORRECTLY
If you could change occupations, which new occupation would you choose ?	92	92.9
What is the name of your favorite restaurant ?	87	87.9
What is the last name of your favorite college instructor ?	97	98.0

TABLE 7

3. Matching of User-Respondent Cognitive Items by Significant-Others

The average number of correct matches by significant-others on all cognitive data questions from the Q2 form was 5.4 out of 20, or 27%. Figure 6-2 reflects the distribution of the correct matches. Again, the distribution approaches that of a normal curve. The distribution curve emphasizes the success rate of the significant-others and is skewed toward the low end of the spectrum. The highest level of success was 10 correct matches (50%) of cognitive data items out of a possible 20. The modal range is 4 to 7 correct responses (20% to 35%). Comparing the distribution of the profile in Figure 6-2 with that in Figure 6-1, there is no overlap. The user-respondents ability to recall cognitive items dwells in the range of 13 to 20 successful matches (out of 20) while the ability of the socially-close significant-others to know how the users would respond gravitates toward the range of zero to 11.

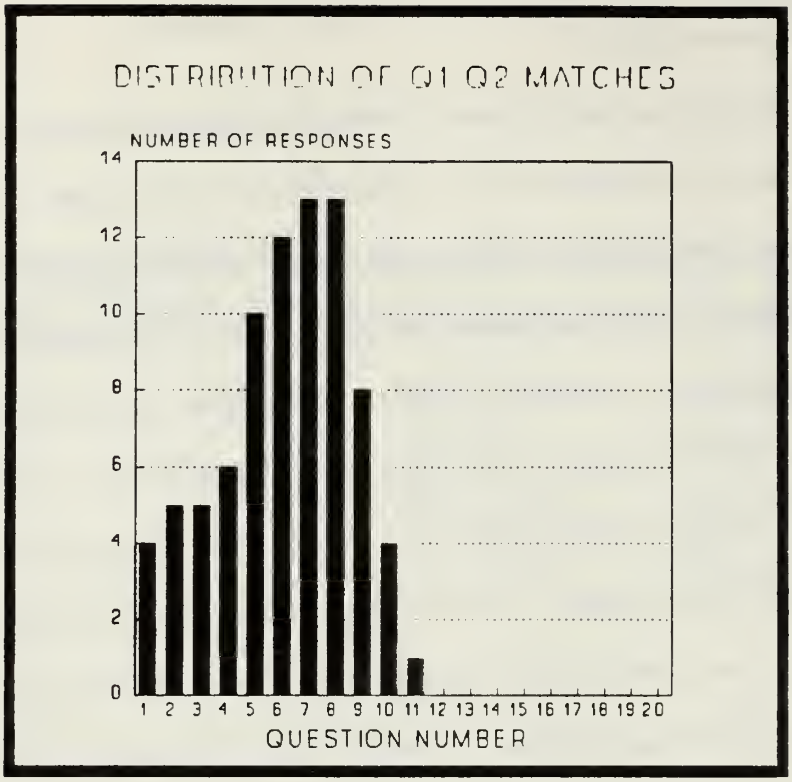

FIGURE 6-2

These significant-other respondents are assumed to be the people closest to the user-respondents: spouses, boyfriends or girlfriends and siblings. Yet, even they do not have correct knowledge, on average, of more than 70% of the items of personal information and personal preferences of the user-respondents.

The difficulty the significant-others had in matching the cognitive data answers of the user-respondents is confirmed in the average percentage score for fact-based cognitive items: 36.9% (Table 8). The assumption was made that the fact-based items would be better known by a socially-close other than would the opinion-based items. The data confirm this assumption as examination of the matches on interest-based and opinion-based items reveals below. Nonetheless, even though the

socially-close others are precisely the people who should know better than anyone else the personal facts about the user-respondents, they knew only about a third of the correct responses.

USER-RESPONDENT MATCHING ON INTEREST-BASED AND OPINION-BASED COGNITIVE DATA ITEMS

ITEM	NUMBER WHO MATCHED CORRECTLY	PERCENT WHO MATCHED CORRECTLY
What is the last name of your favorite actor or actress ?	83	83.8
What is your favorite flower ?	94	94.9
What is your favorite dessert ?	90	90.0
What is your favorite vegetable ?	85	85.9
What is your favorite fruit ?	86	86.9
What is your favorite color ?	95	96.0

TABLE 8

As expected, the significant-others know less about the personal preferences of the user-respondents (Tables 9, 10 and 11) than they know about the user-respondents' personal facts. The average percentage score of matches for the 14 opinion-based items is 22.9%.

An assumption was made that the significant-other respondents are the people in the best position to possess personal knowledge about the user-respondents. The significant-others (spouses, siblings and boyfriends or girlfriends) were assumed, in a social context, to have superior personal knowledge of the user-respondents. Of interest is the ability of gauging just how much personal knowledge is held by socially-close people. A further assumption is that the accuracy of personal knowledge would decrease as soon as even the slightest social distance was introduced.

To examine this social-distance notion of decreasing personal knowledge, the average number of correct matches was calculated on the overall set of 20 cognitive items for the 62 spouses and the 16 friends. The average number of correct matches for spouses was 5.8 (29%); the average for friends was 3.15 (16%). The difference between the two is 54%. To the extent that "friends" can be assumed to be socially more distant than spouses (however slight that might be), the assumption of social-distance affecting personal knowledge has merit.

SIGNIFICANT-OTHER MATCHING ON INTEREST-BASED AND OPINION-BASED COGNITIVE DATA ITEMS

ITEM	NUMBER WHO MATCHED CORRECTLY	PERCENT WHO MATCHED CORRECTLY
What was the name of your favorite class in high school ?	12	14 6
What is the name of your favorite music performer or group ?	24	28 9
What is your favorite type of music ?	26	31.3
What is the name of your favorite vacation place ?	18	21.7
If you could travel to any country in the world, which would it be ?	20	24.1

TABLE 9

SIGNIFICANT-OTHER MATCHING ON INTEREST-BASED AND OPINION-BASED COGNITIVE DATA ITEMS

ITEM	NUMBER WHO MATCHED CORRECTLY	PERCENT WHO MATCHED CORRECTLY
What is the last name of your favorite actor or actress ?	12	14.5
What is your favorite flower ?	28	33.7
What is your favorite dessert ?	18	21.7
What is your favorite vegetable ?	20	24.1
What is your favorite fruit ?	14	16.9
What is your favorite color ?	34	41.0

TABLE 10

SIGNIFICANT-OTHER MATCHING ON INTEREST-BASED AND OPINION-BASED COGNITIVE DATA ITEMS

ITEM	NUMBER WHO MATCHED CORRECTLY	PERCENT WHO MATCHED CORRECTLY
If you could change occupations, which new occupation would you choose ?	11	13.3
What is the name of your favorite restaurant ?	21	25.3
What is the last name of your favorite college instructor ?	8	9.6

TABLE 11

5. Discussion of Findings

a. Recall of Passwords

Over a three-month period, no more than 23.2% of the respondents could recall their system-generated, assigned passwords. This percentage includes the nearly two-thirds of the respondents who wrote down their assigned passwords. This was the case even though the assigned passwords did not exceed seven characters, the accepted limit to human short-term memory (Miller, 1956).

Over the same period, no more than 35.4% of the same respondents could recall the passwords that they had created themselves. Again, this maximum recall included the 14% of the respondents who wrote down their self-generated passwords.

b. Recall of Cognitive Data

After three months, the respondents recalled, on average, 82% of their cognitive passwords. None recalled fewer that 13 (65%) of the 20 cognitive passwords. Over 6% of the respondents recalled all 20 items. When the fact-based cognitive data items was analyzed separately, the recall averaged over 94%. The recall performance on the interest-based and opinion-based cognitive data items was somewhat lower than for the fact-based items. On average, 87.9% of the interest-based and opinion-based items were recalled.

Recall of the cognitive data items was noticeably better than it was for either the assigned or self-generated conventional passwords. Overall, the findings in this study demonstrate an ease of recall for cognitive passwords that is superior to that of conventional passwords.

c. Guessing of Cognitive Data

The people who are socially close to the user-respondents (spouses, close friends and siblings), on average could guess no more than 27% of their users' cognitive data responses. Only one significant-other could guess as many as 10 out of 20 items. The modal responses were six and seven out of the 20. Four significant-others could not guess any of their respondents' choices correctly.

When the guessing of fact-based cognitive items were analyzed separately from interest-based and opinion-based items, the results were as expected. People close to the user-respondents could guess fact-based items better than they could guess interest-based or opinion-base items. On average, the significant-others guessed 36.9% of the fact-based items while averaging only 22.9% for the interest-based and opinion-based cognitive data.

A test of the notion that people more socially close to user-respondents, such as spouses, ought to be better guessers than those even slightly removed, such as close friends and boyfriends or girlfriends showed it to be true. The average number of correct guesses for spouses was 5.8 (29%) compared to 3.15 (16%) for non-spouse significant others.

d. Summary

These findings demonstrate that while cognitive passwords are easy for users to recall, they are difficult for others to guess, even others who are socially close to the users.

VII. IMPLEMENTATION

A. STRUCTURE OF THE COGNITIVE PASSWORD SECURITY MODEL

The cognitive password security model encompasses user password development and a system-generated identification number along with physical security. Implementation is accomplished through two major modules: system administrator and user. These two modules support the two main types of participants in this cognitive password system: a system administrator and one or more users. A brief description of both the system administrator and the user module follows.

1. System Administrator Module

The system administrator module is protected by three layers of security: physical security, segregation from other programs and a unique identification number known only to the system administrator. Access to the system administrator module will only be granted through the system administrator's terminal located in his or her office. This layer of physical security requires any unauthorized user to gain access to the system administrator's office in order to attempt intrusion. Both the system administrator module and the user module were constructed as separate programs so that access to one would not grant access to the other. A unique identification number known only to the system administrator must be entered into the system upon program initiation. In summary three conditions must be met in order to gain access to the system administrator module: access to a particular office, access to the program and knowledge of the unique identification number.

Upon initiating the system administrator module, the system administrator must respond to a query for his or her identification number as illustrated in Figure 7-1.

PLEASE ENTER YOUR ID NUMBER _____
FOLLOWED BY <ENTER>

FIGURE 7-1

When the identification number is entered, it is checked to ensure correctness. If incorrect, an error message is displayed and access is denied. If correct, the System Administrator Main Menu is displayed with its 6 options as shown in Figure 7-2.

```
SYSTEM ADMINISTRATOR - MAIN MENU

A - Add a new user
M - Modify a user's profile
D - Delete a user's profile
V - View a user's profile
U - Unlock a user's profile
E - Exit from system

Select Option ____ and press < ENTER >
```

FIGURE 7-2

a. *Option A - Add a New User*

This option is used to add a new user to the cognitive password system. Upon selection, a random number generator assigns a five digit identification number to the user. After the user is told his or her identification number, the user through the system administrator responds to the 20 question database. In addition, the system administrator sets the account status indicator to active. The status indicator, when set to active or 1, allows a user to access the user module. If set to frozen or 0, a user will not be allowed to use the user module. Figure 7-3 shows a sample of a question display.

WHAT IS THE NAME OF THE ELEMENTARY
SCHOOL FROM WHICH YOU GRADUATED ?

PRESS < ENTER > AFTER ENTERING
ANSWER !

FIGURE 7-3

b. Option M - Modify a User's Profile

Modify is used to change an existing profile. When selected, the system administrator is prompted for a user's identification number. Once a user's profile is located, the system administrator is prompted for the question number to be affected by the change. The question, the current answer and a prompt for a new answer is displayed as shown in Figure 7-4.

```
QUESTION 1 :

  WHAT IS THE NAME OF THE ELEMENTARY
  SCHOOL FROM WHICH YOU GRADUATED ?

  CURRENT ANSWER IS : ____________

  ENTER NEW ANSWER - MAXIMUM OF
 20 CHARACTERS !

PRESS < ENTER > AFTER ENTERING !
```

FIGURE 7-4

c. *Option D - Delete a User's Profile*

Delete is used to remove a user's profile from the cognitive password database. Reasons for removal may be that a user no longer requires access or that a user is no longer associated with the organization. The system administrator selects the delete option and is prompted for a user's identification number. When the specific account is located, its identification number and its answer database is removed from the password database as illustrated in Figure 7-5.

FIGURE 7-5

d. Option V - View a User's Profile

View is used to display the answer database for a particular user. The system administrator is prompted for a user's identification number. When located, a user's entire account is displayed as shown in Figure 7-6. No modifications can be made from this option.

```
              USER _____ PROFILE

        STATUS        --
        ANSWER 1       -----------------
        ANSWER 2       -----------------
        ANSWER 3       -----------------
        ANSWER 4       -----------------
        ANSWER 5       -----------------
        ANSWER 6       -----------------
        ANSWER 7       -----------------
        ANSWER 8       -----------------
        ANSWER 9       -----------------
        ANSWER 10      -----------------
        ANSWER 11      -----------------
        ANSWER 12      -----------------
        ANSWER 13      -----------------
        ANSWER 14      -----------------
        ANSWER 15      -----------------
        ANSWER 16      -----------------
        ANSWER 17      -----------------
        ANSWER 18      -----------------
        ANSWER 19      -----------------
        ANSWER 20      -----------------
```

FIGURE 7-6

e. Option U - Unlock a User's Profile

Unlock is used to change the account status indicator. If the status indicator is set to 0, the account is frozen and access to the user module is not allowed. If set to 1, the account is active and access is allowed to the user module. The account status indicator can be set at three times: when adding a new user, when modifying the profile of an existing user and when a user has failed after two attempts to furnish the appropriate answers to the questions asked in the user module. The unlock option is used by the system administrator to reactivate an account. When selected, the system administrator is prompted for a user's identification number. After

locating a user's file, the current status indicator is displayed along with the option of changing it as shown in Figure 7-7.

CURRENT STATUS = __

DO YOU WANT TO CHANGE THE STATUS ?

Y or N

PRESS < ENTER > AFTER SELECTING !

FIGURE 7-7

f. Option E - Exit from System

Exit is used to save all records and exit from the cognitive password system. When selected, all records are written to the database and the user is asked if he or she wishes to return to the System Administrator Main Menu. If a user answers "no", control is returned to the operating system. Figure 7-8 shows the exit screen.

ALL RECORDS HAVE BEEN SAVED !

DO YOU WANT TO GO BACK TO THE
MAIN MENU ? Y or N

PRESS < ENTER > AFTER SELECTING !

FIGURE 7-8

2. User Module

After a user has established his or her account, a user will interface only with the user module. The only exceptions would be if a user's account is frozen or if a user desired to modify an answer.

The first test faced by a user attempting to gain access through the user module is to enter his or her identification number. When entered, the identification number is checked for correctness. If incorrect, a user is given additional opportunities to enter the correct number. If correct, a user proceeds to the question and answer phase. A maximum of two attempts is allowed before the respective account is frozen.

a. Attempt One

When a user's identification number is evaluated as correct, he or she is instructed that five questions will be asked as shown in Figure 7-9. After this informational screen is displayed, five randomly selected questions are selected and displayed one at a time, Figure 7-10. A user responds to each question. After all 5 questions have been answered, the responses are compared to the answers stored in the answer database. If correct, access is granted, Figure 7-11. If incorrect, access is denied, Figure 7-12, and the user proceeds to the second attempt. No error messages are given to indicate if any answers are incorrect. This is a security feature to prevent a potential intruder from attempting to guess the appropriate answers.

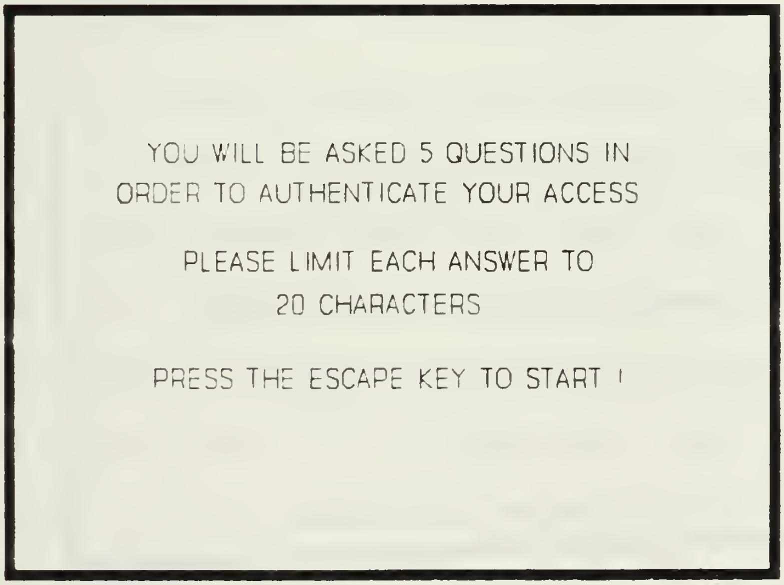

FIGURE 7-9

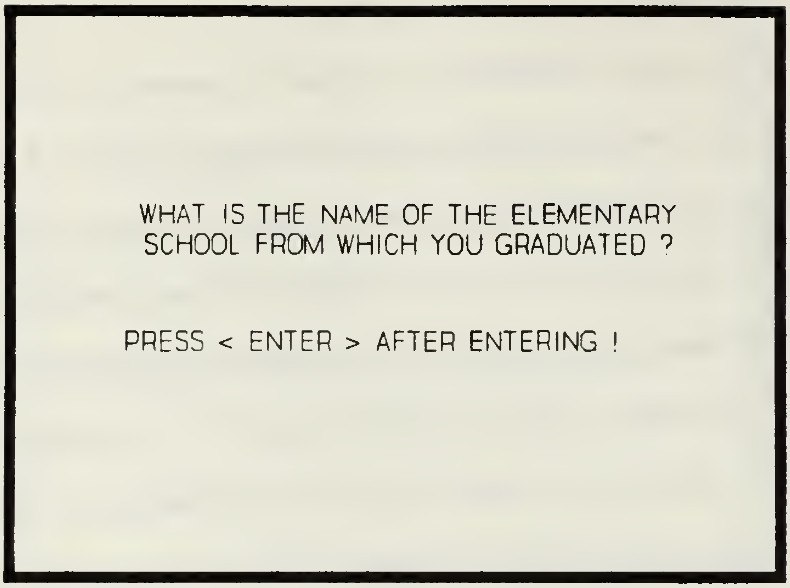

FIGURE 7-10

FIGURE 7-11

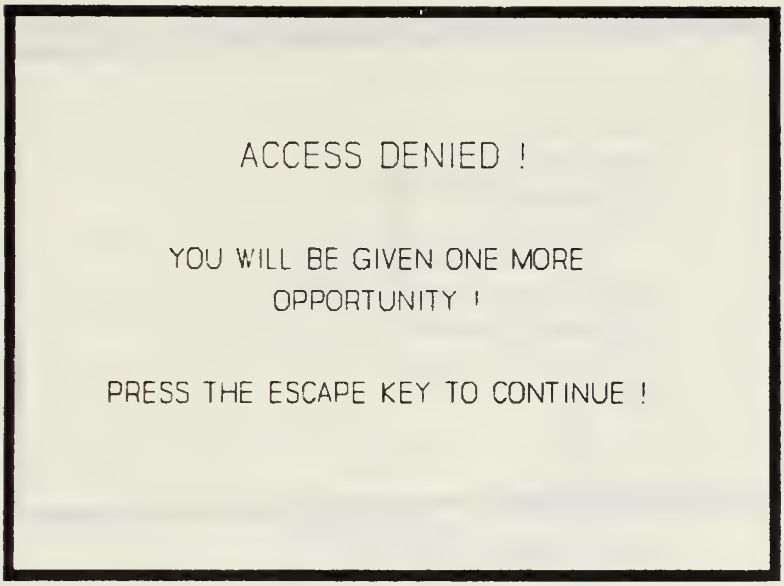

FIGURE 7-12

b. Attempt Two

Five questions are randomly selected from the question database. Safeguards have been built into the cognitive password system to ensure there will be no duplication of questions between attempt 1 and attempt 2. Each question is asked in the same fashion as in attempt 1, Figure 7-10. After responses are obtained, each answer is compared against the respective answers stored in the answer database. If correct, access is granted, Figure 7-11. If incorrect, four actions occur: access is denied, the account is frozen by automatically changing the account status indicator to 0, the user is instructed to contact the system administrator before attempting further use and the user is exited from the system. Figure 7-13 illustrates the access denial display.

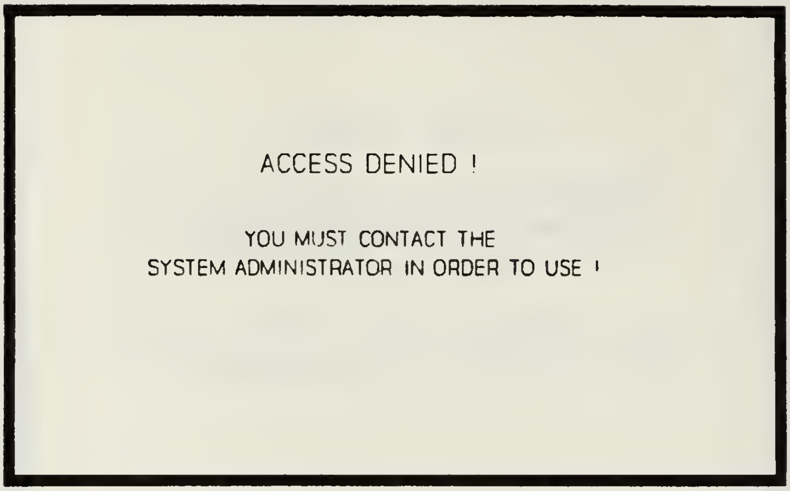

FIGURE 7-13

Figure 7-14 summarizes the logic of the user module.

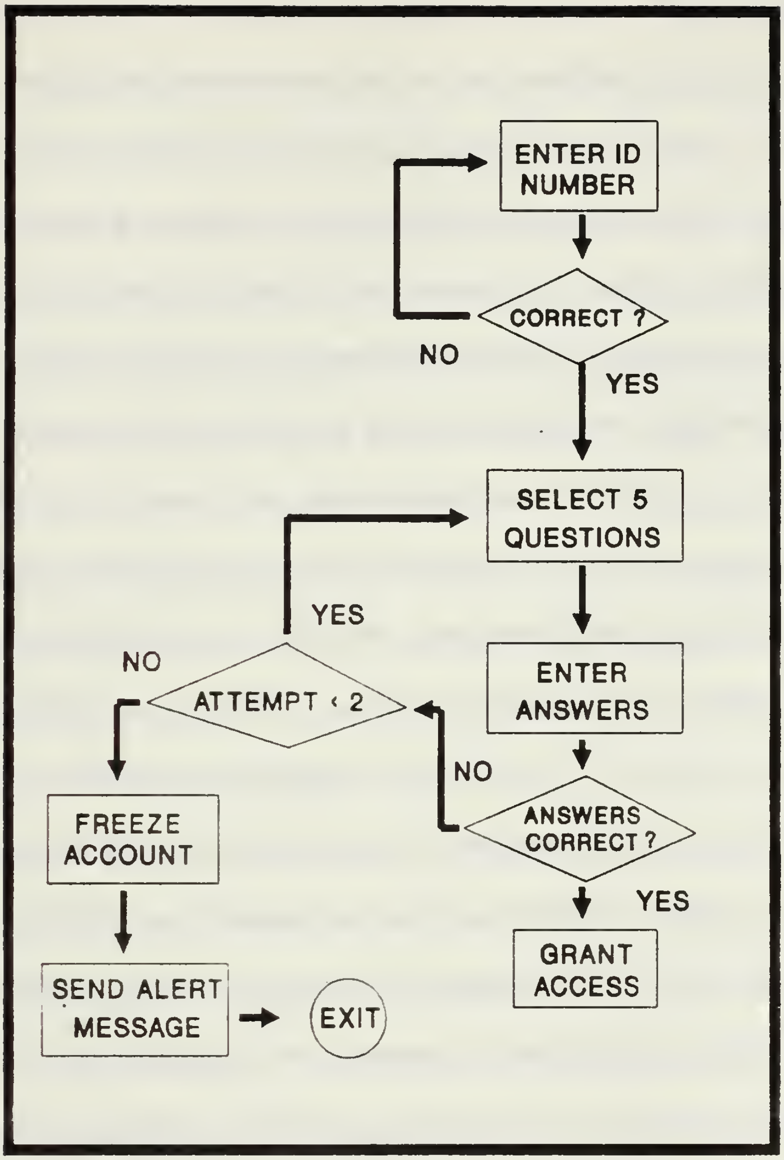
ENTER ID
NUMBER
CORRECT ?
NO
YES
SELECT 5
QUESTIONS
YES
NO
ATTEMPT < 2
ENTER
ANSWERS
NO
ANSWERS
CORRECT ?
YES
FREEZE
ACCOUNT
GRANT
ACCESS
SEND ALERT
MESSAGE
EXIT

FIGURE 7-14

3. Sample Case

The system administrator is the focal point of a security system. If a system is large enough, a systems administrator may delegate specific functions to assistants, such as a systems security manager. While a security manager is primarily responsible for the security of a computerized system, the system administrator remains overall responsible. In this discussion and in the following example, a system administrator retains all responsibilities and therefore, is the primary point of contact.

Initially, a potential user meets with the system administrator in the administrator's office to start a sequence of events culminating in a user being granted access to the system as an authorized user. The first order of business is to verify a user's need to access the information system. Verification should be obtained independently of a user; i.e., a potential user should not be allowed to furnish his or her own verification. An ideal scenario is for verification of need to be accomplished prior to an initial meeting. If unable to do so, a potential user should not be granted an interview until verification is satisfactory. Proof of need may take various forms: a written or electronic request from a potential user's department head transmitted independently of a potential user or a valid organizational identification card matched with an authorized request such as a validated course enrollment form. After this initial step is complete, step 2, familiarization with appropriate rules and regulations, takes place.

A list of do's and don'ts should be compiled in layman's terms. Each potential user should be required to read this list and ask any questions he or she desires. Once a potential user understands the rules and regulations, he or she should

sign acknowledging understanding and receipt of a copy. Only after the systems administrator has verified need and is satisfied that the potential user understands the procedures, should a potential user be recognized as a new user.

At this stage, step 3, the systems administrator will activate the system administrator module and initiate the user's profile. An identification number is generated and assigned and the responses to the 20 questions in the question database are entered into the answer database. Each answer is given verbally, thereby eliminating the need to commit any answers to paper. By elimination of paper media, the risk of a user committing any of the answers to writing is reduced. This security safeguard helps ensure that the password answers will not transition to something possessed as opposed to something known. Upon completion of this step, a user is now authorized to use the user module.

Step 4 is the user log-in process. When a user activates a terminal, the cognitive password system is automatically accessed. A user will be first asked to enter his or her identification number. If the identification number is not valid, the user will receive additional opportunities to enter the correct identification number. If correct, the user will be asked five questions. The responses to these questions are compared to the stored answers asked at the time the user first initiated his or her profile. If the answers match, access is granted. If incorrect, the user is asked five additional questions. Again the responses to the second set of questions are compared to the stored answers. If correct, access is granted. If incorrect, access is denied, the account is frozen and the user is exited from the system. Further use of the computer system is denied until the unsuccessful user meets with the system administrator.

VIII. CONCLUSIONS AND RECOMMENDATIONS

A. YES! THERE IS A BETTER WAY!

In Chapter IV, the question "Is there a better way?" was asked concerning passwords. The foregoing research confirms that passwords can be made to be more effective and yield a high degree of security.

1. The Inadequacy of Traditional Passwords

This study outlines the problems found in traditional passwords: hard to remember, easy to guess, written down on paper, low level of security provided and user resistance. At the same time that traditional passwords were being criticized, they remained the most common form of computer access control.

Traditional passwords have not kept up with the rapid advances in information systems technology. The widespread proliferation of networks and users' desires to be able to access computer systems from basically anywhere in the world has caused traditional passwords to fall from favor. While still widely used, users have decreasing confidence in their capability to provide adequate security. The need to find a better password has brought password variations such as cognitive passwords to the forefront.

2. Advantages of Cognitive Passwords

This research has shown that cognitive passwords indeed offer several advantages over traditional passwords.

a. *User Selection*

Cognitive passwords allow a user to select the password. As has been shown, user selected passwords enjoy a high degree of memorability and low user resistance. The survey conducted with this study confirms this advantage. Of the test group, 23.2% could recall the system generated assigned password, 35.4% could recall the user selected password and 82% could recall their cognitive password. This marked increase in ability to recall portends well for cognitive passwords.

b. *Difficulty of Guessing*

A goal of any security system is to deter potential intruders from attempting to gain entry through guessing. Cognitive passwords demonstrate that indeed they are difficult to guess. People that are socially close to the user-respondents could guess only 27% of the cognitive passwords. People that could be assumed to be the closest to the user-respondents, spouses, fared little better. They could only guess correctly 29% of the time. The assumption that people not socially close to the user-respondents, such as friends, would have an even more difficult time in guessing cognitive passwords were confirmed by this research. Friends could only guess 16% of the cognitive passwords.

c. *Ease of Memorability*

The degree of memorability correlates directly with the ease of guessing. Users tend to select easy to remember passwords, primarily meaningful items or details. The classic examples are spouses' names or birthday dates. While easy to remember, the passwords were unfortunately easy to guess. Little effort is needed to guess the traditional password. As stated in section (a) above, the marked increase in

the degree of recall of cognitive passwords compared to system generated or user selected passwords is significant.

d. *Use of Episodic Memory*

Research into the development of effective passwords indicate that passwords based on episodic memory are most effective. The advantage of episodic memory is that it is based on meaningful details that is mostly unshared with anyone else. Cognitive passwords are built upon this premise. Unshared memory is more difficult to guess and would not normally be written down in personnel files. Barton (1984) indicated that good formulation produces passwords that are distanced enough in form from ordinary experience to make compromise unlikely. Cognitive passwords are based on items and details known normally to the user.

e. *Construction*

Menkus (1988), Fisher (1983) and Kurzban (1983) listed three characteristics that directly affected good construction of passwords: length, character set and memorability.

(1) Length. The longer the password, the more difficult it is to guess, and therefore the more secure it is (Wood, 1983). A cognitive password system based on 20 questions each of a maximum length of 20 characters yields a robust base.

(2) Character Set. While passwords constructed of random characters yield the highest degree of security, practicality dictates character sets that can be remembered. The most common solution to this problem is the addition of vowels to characters to make the password memorable and therefore easier to use. The larger the character set, the larger the number of possible combinations. Length coupled with

the character set determine how robust a password will be. The current implementation of a cognitive password system has sufficient length and character set to yield a robust, effective security system.

(3) Memorability. As previously stated, cognitive passwords have been demonstrated to be easier to recall than either system generated or user selected passwords. One factor that greatly improves memorability is the ability of a user to construct his or her own password. As has already been shown, cognitive passwords take advantage of this user selection. In fact, cognitive passwords combines the advantages of user selection and a user's innate desire to select meaningful details. The synergism of user selection and meaningful details yields a rich and effective password security system.

3. Degree of Security

The degree of security provided by any password system is a function of user acceptance. If a system is difficult, the system will be either not used or circumvented. Cognitive password systems offer the advantages of high memorability, ease of use, user selection and little user resistance.

4. Implementation of a Cognitive Password System

How difficult would a cognitive password system be to implement? As part of this study, a prototype of such a system was built and implemented. The prototype was coded in Pascal and designed for a stand-alone microcomputer. The system was found to be easy to understand, inexpensive to implement and easy to maintain. Adaptation of this prototype to a network, a minicomputer or a mainframe computer could be accomplished with a minimum of effort.

5. Summary

Cognitive passwords have been shown to be an effective computer security mechanism. Ahituv, Lapid and Neumann's evaluation model relative to cognitive passwords is illustrated in Figure 8-1.

EVALUATION OF THE
COGNITIVE PASSWORD MODEL

CRITERIA	MODEL
1. EASILY REMEMBERED ?	YES
2 HARD TO GUESS BY ASSOCIATION ?	YES
3. EASY TO KEY- IN ?	YES
4. ATTACKABLE BY SPOOFING OR TROJAN HORSE ?	YES
5 TESTED ?	YES
6. EASY TO IMPLEMENT ?	YES
7. COST PROHIBITIVE ?	NO

FIGURE 8-1

B. RECOMMENDATIONS

This study shows that cognitive password systems can be an effective computer security mechanism. Further research into cognitive passwords is recommended. Closely related to cognitive passwords, is the area of associative passwords. Smith (1987) has conducted preliminary research in this area. Research into how associative passwords relate to cognitive passwords is recommended.

APPENDIX

THESIS QUESTIONNAIRE QI - COGNITIVE PASSWORDS

BACKGROUND: The purpose of this questionnaire is to develop a sample database of appropriate questions and answers to be utilized in developing a prototype of a cognitive password system.

PART A: PERSONAL INFORMATION

Please answer the following questions:

Age ______

Gender: Female____, Male____

Last four digits of SSN ________

Number of years experience, if any, in computer usage: ____

Type of computer(s) used prior to NPS (check any that apply):
- a. Microcomputer ____
- b. Microcomputer linked to a mainframe ____
- c. Mainframe terminal ____

PART B: PASSWORDS

1. Please construct and write in the space provided below your own password, up to 8 characters (letters and/or numbers). Try to memorize and safeguard it as you would any other password.

|__|__|__|__|__|__|__|__|

2. How did you choose your password in (1) above?
   - a. A meaningful detail (name, date, number, etc.) ____
   - b. A combination of meaningful details ____
   - c. A randomly chosen combination of characters ____
   - d. Other (Please specify) _______________

3. The following password has been assigned to you for this study. Please memorize and safeguard it as you would any other password.

|__|__|__|__|__|__|__|__|

PART C: Cognitive Questions For Passwords

Please answer all questions with a maximum of 20 characters.

1. What is the name of the elementary school from which you graduated ? _______________
2. What is the first name of your favorite uncle ? ____________
3. What is the first name of your best friend in high school? _______________
4. What is your mother's maiden name? _______________
5. What was the first name of your first boyfriend/girlfriend? _______________
6. What was the name of your favorite class in high school? _______________
7. What is the name of your favorite music performer or group? _______________
8. What is your favorite type of music? _______________
9. What is the name of your favorite vacation place? ___________
10. If you could travel to any country in the world, which would it be? _______________
11. What is the last name of your favorite actor or actress? _______________
12. What is your favorite flower? _______________
13. What is your favorite dessert? _______________
14. What is your favorite vegetable? _______________
15. What is your favorite fruit? _______________
16. What is your favorite color? _______________
17. If you could change occupations, which new occupation would you choose? _______________
18. What is the name of your favorite restaurant? _______________

19. What is the occupation of your father? _______________

20. What is the last name of your favorite college instructor?

____

THESIS QUESTIONNAIRE Q2 - COGNITIVE PASSWORDS

Last four digits of SSN ______, Relationship __________

BACKGROUND: The purpose of this questionnaire is to develop a sample database of appropriate questions and answers to be utilized in developing a prototype of a cognitive password system. Please try to answer the following questions **REGARDING THE PERSON WHO GAVE YOU THIS QUESTIONNAIRE,** without his/her help.

Please answer the following questions with a maximum of 20 characters. Leave blank if you don't know the answer!

1. What is the name of the elementary school from which he/she graduated ?

   ____

2. What is the first name of his/her favorite uncle ? ___________
3. What is the first name of his/her best friend in high school?

   ____

4. What is his/her mother's maiden name? ______________
5. What was the first name of his/her first boyfriend/girlfriend?

   ____

6. What was the name of his/her favorite class in high school?

   ____

7. What is the name of his/her favorite music performer or group?

   ____

8. What is his/her favorite type of music? ______________
9. What is the name of his/her favorite vacation place? ________
10. If he/she could travel to any country in the world, which would it be? ______________
11. What is the last name of his/her favorite actor or actress?

    ____

THESIS QUESTIONNAIRE Q2 - COGNITIVE PASSWORDS

12. What is his/her favorite flower? _______________

13. What is his/her favorite dessert? _______________

14. What is his/her favorite vegetable? _______________

15. What is his/her favorite fruit? _______________

16. What is his/her favorite color? _______________

17. If he/she could change occupations, which new occupation would he/she choose?

    ____

18. What is the name of his/her favorite restaurant? _________________

19. What is the occupation of his/her father? _______________

20. What is the last name of his/her favorite college instructor?

    ____

THESIS QUESTIONNAIRE Q3 - COGNITIVE PASSWORDS

BACKGROUND: The purpose of this questionnaire is to determine how well a person can remember the answers previously given in the first questionnaire. Please answer to the best of your ability.

PART A: PERSONAL

Last four digits of SSN ________

PART B: PASSWORDS

1. Please write in the space below the password you developed and wrote on the first questionnaire.

|__|__|__|__|__|__|__|__|

2. How did you remember your password in (1) above? Please be honest!

a. Committed to memory ____
b. Wrote on paper ____

3. On the first questionnaire, you were assigned a password. Please write that password in the space below.

|__|__|__|__|__|__|__|__|

4. How did you remember your password in (3) above?

a. Committed to memory ____
b. Wrote on paper ____

PART C: Cognitive Questions For Passwords

The following questions were asked in the first questionnaire.
Please answer all questions with a maximum of 20 characters.

1. What is the name of the elementary school from which you graduated ?

____

2. What is the first name of your favorite uncle ? ____________

3. What is the first name of your best friend in high school?

____

4. What is your mother's maiden name? _______________
5. What was the first name of your first boyfriend/girlfriend? _______________
6. What was the name of your favorite class in high school? _______________
7. What is the name of your favorite music performer or group? _______________
8. What is your favorite type of music? _______________
9. What is the name of your favorite vacation place? ___________
10. If you could travel to any country in the world, which would it be? _______________
11. What is the last name of your favorite actor or actress? _______________
12. What is your favorite flower? _______________
13. What is your favorite dessert? _______________
14. What is your favorite vegetable? _______________
15. What is your favorite fruit? _______________
16. What is your favorite color? _______________
17. If you could change occupations, which new occupation would you choose? _______________
18. What is the name of your favorite restaurant? _______________
19. What is the occupation of your father? _______________
20. What is the last name of your favorite college instructor? _______________

LIST OF REFERENCES

Ahituv, N., Lapid, Y., and Neumann, S., "Verifying the Authentication of an Information System User", *Computers and Security*, Vol. 6, No. 2, pp. 152-157, 1987.

Avarne, S., "How to Find Out a Password", *Data Processing & Communications Security*, Vol. 12, No. 2, pp. 16-17, Spring 1988.

Barton, B.F., and Barton, M.S., "User-Friendly Password Methods for Computer-Mediated Information Systems", *Computers and Security*, Vol. 3, No. 3, pp. 186-195, 1984.

Department of Defense Computer Security Center CSC-STD-002-85, *Department of Defense Password Management Guidelines*, 1985.

Fisher, R.P., *Information Systems Security*, pp. 97-120, Prentice-Hall, Inc., 1984.

Hagopian, G., "Planning and Implementing a Security Package", *Data Processing & Communications Security*, Vol. 11, No. 1, pp. 10-11, Winter 1987.

Hsiao, D.K., Kerr, D.S., and Madnick, S.E., *Computer Security*, pp. 43-105, Academic Press, 1979.

Kaiser, W.G., "The Making of a B2 System", *Data Processing & Communications Security*, Vol. 11, No. 1, pp. 19-23, Winter 1987.

Kurzban, S., "A Dozen Gross 'Mythconceptions' About Information Processing Security", *Security, IFIP*, pp. 15-25, 1983.

Martin, J., *Security, Accuracy and Privacy in Computer Systems*, pp. 127-141, Prentice-Hall, Inc., 1973.

Menkus, B., "Understanding the Use of Passwords", *Computers and Security*, Vol. 7, No. 2, pp. 132-136, April 1988.

Miller, G.A., "The Magical Number Seven, Plus or Minus Two: Some Limits on Our Capacity for Processing Information", *The Psychological Review*, Vol.63, pp. 81-97, March 1956.

Panns, R., and Herschberg, I.S., "Computer Security: The Long Road Ahead", *Computers and Security*, Vol. 6, No. 5, pp. 403-416, 1987.

Pfleeger, C.P., *Security in Computing*, pp. 75-83, Prentice-Hall, Inc., 1989.

Porter, S.N., "A Password Extension for Improved Human Factors", *Computers and Security*, Vol. 1, No. 1, pp. 54-56, 1982.

Smith, S.L., "Authenticating Users by Word Association", *Computers and Security*, Vol. 6, No. 6, pp. 464-470, 1987.

Spender, J.C., "Identifying Computer Users with Authentication Devices (Tokens)", *Computers and Security*, Vol. 6, No. 5, pp. 385-395, 1987.

Wood, C.C., "Effective Information System Security with Password Controls", *Computers and Security*, Vol.2, No. 1, pp. 5-10, 1983.

INITIAL DISTRIBUTION LIST

1.	Defense Technical Information Center Cameron Station Alexandria, VA 22304-6145	2
2.	Library, Code 0142 Naval Postgraduate School Monterey, CA 93943-5002	2
3.	Moshe Zviran, Code 54ZV Naval Postgraduate School Monterey, CA 93943-5000	1
4.	William J. Haga, Code 54HA Naval Postgraduate School Monterey, CA 93943-5000	1
5.	LT John D. Hulsey c/o Howard A. Webb 4200 Kimball Bridge Road Alpharetta, GA 30201	2